EVALUASI KESIAPAN KERANGKA KERJA KEAMANAN INFORMASI PADA DINAS KOMUNIKASI DAN INFORMATIKA KOTA BATU DENGAN MENGGUNAKAN INDEKS KAMI

SKRIPSI

Untuk memenuhi sebagian persyaratan
Memperoleh gelar Sarjana Komputer

Disusun oleh:
Shella Indah Dwi Octaviani
NIM: 155150401111099

PROGRAM STUDI SISTEM INFORMASI
JURUSAN SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2018

PENGESAHAN

EVALUASI KESIAPAN KERANGKA KERJA KEAMANAN INFORMASI PADA DINAS KOMUNIKASI DAN INFORMATIKA KOTA BATU DENGAN MENGGUNAKAN INDEKS KAMI

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun Oleh :
Shella Indah Dwi Octaviani
NIM: 155150401111099

Skripsi ini telah diuji dan dinyatakan lulus pada
28 Desember 2018
Telah diperiksa dan disetujui oleh:

Dosen Pembimbing I	Dosen Pembimbing II
Suprapto, S.T, M.T	Adhitya Dwi Herlambang, S.Pd., M.Pd.
NIK: 19710727 199603 1 001	NIK: 2016098908021001

Mengetahui
Ketua Jurusan **Sistem Informasi**

Dr. Eng. Herman Tolle, S.T, M.T
NIP. 19740823 200012 1 001

PERNYATAAN ORISINALITAS

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, di dalam naskah skripsi ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis disitasi dalam naskah ini dan disebutkan dalam daftar pustaka.

Apabila ternyata didalam naskah skripsi ini dapat dibuktikan terdapat unsurunsur plagiasi, saya bersedia skripsi ini digugurkan dan gelar akademik yang telah saya peroleh (sarjana) dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku (UU No. 20 Tahun 2003, Pasal 25 ayat 2 dan Pasal 70).

Malang, 18 Desember 2018

Shella Indah Dwi Octaviani
NIM: 155150401111099

iii

PRAKATA

Segala puji bagi Allah SWT, karena atas Rahmat dan Hidayah-Nya penulis dapat menyelesaikan skripsi dengan judul "Evaluasi Kesiapan Kerangka Kerja Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Batu Dengan Menggunakan Indeks KAMI". Penulisan skripsi ini merupakan salah satu syarat untuk mendapatkan gelar sarjana komputer pada Fakultas Ilmu Komputer Universitas Brawijaya. Dalam penyusunan skripsi ini banyak pihak yang telah membantu dan memberikan dukungan, perkenankan penulis menyampaikan terima kasih kepada :

1. Bapak Suprapto selaku dosen pembimbing satu dan Bapak Admaja Dwi Herlambang selaku dosen pembimbing dua yang telah memberikan ilmu, saran, motivasi dan do'a untuk kelancaran pengerjaan skripsi ini.
2. Bapak Yusi Tyroni Mursityo selaku Ketua Prodi Sistem Informasi Fakultas Ilmu Komputer Universitas Brawijaya.
3. Bapak Herman Tolle selaku Ketua Jurusan Sistem Informasi Fakultas Ilmu Komputer Universitas Brawijaya.
4. Bapak Wayan Firdaus Mahmudy selaku Dekan Fakultas Ilmu Komputer Universitas Brawijaya.
5. Bapak Bapak Riski Yuniar, Bapak Cahya Wisesa, dan Bapak Robert yang telah mengizinkan penulis untuk melakukan wawancara, observasi dan penyebaran kuesioner dalam melakukan penelitian pada Dinas Komunikasi dan Indah Kota Batu.
6. Kedua orangtua, ayahanda Mardiyana dan Ibunda Sriyuliani. Saudara penulis, yaitu Rendy Eka Bagus dan Irmas Kharismya. Keponakan penulis, yaitu Danish Hamizan Putra serta seluruh keluarga besar penulis yang tak henti-hentinya memberikan semangat, doa, dan dukungan selama proses pengerjaan skripsi.
7. Muhammad Harist yang tidak pernah berhenti memberikan dukungan, semangat, dan motivasi dari jauh kepada penulis dalam bentuk apapun.
8. Ratna Dwi, Widhi Asih, Nina Dian, Rifdah Nur Fadhilah, Devita Widyasari, Dimitri Yola, Theresia Emiliana, Despa Siswanti dan Nanda Fiesta yang tidak pernah berhenti memberikan dukungan, semangat dan motivasi kepada penulis dalam bentuk apapun.
9. Segenap teman-teman Eksekutif Mahasiswa Sistem Informasi 2017/2018 dan Eksekutif Mahasiswa Sistem Informasi 2018/2019. Terima kasih atas pengalaman berharganya selama penulis kuliah di Universitas Brawijaya.
10. Segenap mahasiswa Program Studi Sistem Informasi Fakultas Ilmu Komputer Universitas Brawijaya tahun 2015. Terima kasih telah memberikan pengalaman berharga dan bantuan untuk penulis.
11. Kepada semua pihak yang tidak dapat penulis sebutkan satu-persatu yang telah membantu kelancaran dalam penyelesaian skripsi ini.

Semoga segala kebaikan dan bantuan dari semua pihak yang telah diberikan kepada penulis mendapatkan balasan dan rahmat dari Allah SWT. Penulis menyadari sepenuhnya bahwa dalam skripsi ini masih jauh dari kata sempurna. Oleh karena itu, penulis mengharapkan kritik dan saran pembaca sebagai sarana untuk menyempurnakan skripsi ini. Semoga skripsi ini dapat bermanfaat bagi pembaca secara umum dan penulis secara khusus.

Malang, 18 Desember 2018

Penulis,
shellaindahdo@gmail.com

ABSTRAK

Shella Indah Dwi Octaviani, Evaluasi Kesiapan Kerangka Kerja Keamanan Informasi Pada Dinas Komunikasi dan Informatika Kota Batu Dengan Menggunakan Indeks KAMI

Pembimbing : Suprapto, S.T, M.T dan Admaja Dwi Herlambang, S.Pd., M.Pd

Pada Pemerintah Kota Batu terdapat satu dinas yang bergerak dalam bidang komunikasi dan informatika serta menyediakan layanan publik yaitu Dinas Komunikasi dan Informatika. Dinas Komunikasi dan Informatika Kota Batu memerlukan evaluasi terhadap keamanan informasi. Sebagai penyedia informasi, Dinas Komunikasipdan Informatika Kota Batu memerlukan evaluasi tingkat keamanan informasi. Pada penelitian ini evaluasi dilakukan dengan instrumen kuesioner berdasar pada IndekspKemananan Informasi (KAMI) untuk melihat hasil kelengkapan dan kematangan keamanan informasi pada 5 area, tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan aset, dan teknolongi. Dari hasil evaluasi diketahui bahwa untuk tingkat kelengkapan mendapatkan skor 203 danprata-rata tingkat kematangan setiap area keamanan informasi berada pada Level I sampai Level I+. Hal ini menyatakan bahwa Dinas Komunikasi dan Informatika Kota Batu dinyatakan tidak layak untuk melakukan sertifikasi ISO 27001. Rekomendasipdidapatkan dari hasil perbandingan antara Indeks KAMI dengan kontrol pada ISO 27001. Rekomendasi yang dapat diberikan kepada Dinas Komunikasi dan Informatika Kota Batu salah satunya harus membuat kebijakan terkait keamanan informasi berdasarkan kontrol objektif A.5.1 pada ISO 27001.

Kata kunci: evaluasi, keamanan informasi, Indeks KAMI, ISO 27001:2013

ABSTRACT

Shella Indah Dwi Octaviani, ***Framework Evaluation of Information Security at Department of Communication and Informatics of Batu City Using Information Security Indeks (KAMI)***

Pembimbing : Suprapto, S.T, M.T dan Admaja Dwi Herlambang, S.Pd., M.Pd

In the Batu City Government there is one office that is engaged in communication and informatics and provides public services, namely the Department of Communication and Informatics. Department of Communication and Informatics of Batu City requires an evaluation of information security. As an information provider, the Department of Communication and Informatics of Batu City requires an evaluation of the level of information security. In this study evaluation was conducted with a questionnaire instrument based on the Information Security Index (KAMI) to see the results of the completeness and maturity of information security in 5 areas, governance, risk management, frameworks, asset management, and technology. From the evaluation results, it is known that for completeness levels get a score of 203 and the average maturity level of each information security area is at Level I to level I +. This states that the Department of Communication and Informatics of Batu City was declared not feasible to carry out ISO 27001 certification. Recommendations were obtained from the results of comparisons between Index of Information Security and controls of ISO 27001. One recommendation that could be given to the Batu Communication and Information Office was to make a policy for information security base on objective control A.5.1 in ISO 27001.

Keywords: evaluation, information security, information security index, ISO 27001:2013

DAFTAR ISI

DAFTAR TABEL

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Pada masa sekarang ini teknologi informasi yang terus berkembang pesat bukan lagi menjadi hal baru untuk dibicarakan. Perkembangan teknologi informasi (TI) ini dapat mempermudah pengguna TI dalam memperolah data dan informasi secara cepat. Menurut Tata Sutabri (2012) informasi adalah data yang digunakan untuk pengambilan keputusan dan telah dikelompokan untuk digunakan dalam proses pengambilan keputusan. Oleh karena itu informasi merupakan aset yang sangat berharga, baik untuk perseorangan, pemerintah maupun swasta. Informasi memiliki nilai dan harus dilindungi, sehingga menjadi penting bagi individu untuk melakukan perlindungan terhadap informasi untuk menghindari penyalahgunaan dari suatu informasi tersebut.

Seiring dengan perkembangan teknologi informasi seluruh organisasi atau perusahaan harus selalu beradapatasi serta mengimplementasikan kemajuan TI. Tuntutan untuk menyelenggarakan *e-government* membuat intansi pemerintah menerapkan teknologi informasi untuk membantu mereka dalam menyelesaikan tugas dan memberikan pelayanan kepada masyarakat. Salah satu instansi pemerintah yang menggunakan teknologi informasi adalah Dinas Komunkasi dan Informatika Kota Batu. Dinas Komunikasi dan Informatika Kota Batu merupakan salah satu perangkat daerah yang memiliki tugas membantu Walikota untuk mengelola urusan pemerintah yang menjadi kewenangan daerah di bidang komunikasi dan informatika.

Pada Rencana Kerja (RENJA) tahun 2018, Dinas Komunikasi dan Informatika Kota Batu telah merumuskan suatu tujuan yaitu “Membangun pola pikir masyarakat Kota Wisata Batu yang cerdas, mandiri, dan berbudaya dengan pemanfaatan teknologi informasi dan komunikasi”. Dalam mewujudkan tujuannya Dinas Komunikasi dan Informatika Kota Batu menetapkan sasaran jangka menengahnya yaitu meningkatnya pemanfaatan data dan informasi yang aktual dan terukur, meningkatnya penyebaran informasi publik melalui media cetak dan media elektronik serta meningkatnya pengelolaan sistem informasi berbasis teknologi yang efektif dan efisien. Untuk mencapai tujuan yang sesuai sasaran jangka menengahnya maka Dinas Komunikasi dan Informatika Kota Batu telah mempunyai beberapa sistem, diantaranya yaitu terdapat sistem informasi Among Tani yang digunakan untuk mengedukasi petani dan sebagai sarana bagi petani untuk menjual hasil panennya; Among Kota merupakan sistem informasi yang berguna untuk memberikan informasi terkait pariwisata, berita, *event* dan lain-lain di Kota Batu; Among Warga merupakan sistem informasi yang digunakan untuk memfasilitasi antara masyarakat dengan pemerintahan, seperti masalah kemacetan, lalu lintas, tanah longsor, dan lain-lain; serta masih banyak lagi teknologi informasi yang digunakan Dinas Komunikasi dan Informatika Kota Batu. Sebagai sarana dalam menyimpan dan mengelola data dari

sistem – sistem yang dijalankannya, Dinas Komunikasi dan Informatika Kota Batu memiliki *server center. Server center* berisi informasi yang penting dan berharga yang menyangkut data pribadi dan rahasia, informasi penting yang dilindungi terkait Bidang Keuangan; Bidang Kesehatan; Bidang Kearsipan; Bidang Kependudukan; Bidang Kepegawaian; Bidang Sosial; Bidang Komunikasi dan Informatika; Bidang Perekonomian; Bidang Hukum dan Peraturan; dan Bidang Persandian dan Telekomunikasi, maka dari itu diperlukan suatu keamanan dengan standar yang pasti.

Berdasarkan hasil wawancara yang telah dilakukan oleh peneliti terhadap Dinas Komunikasi dan Informatika Kota Batu, narasumber menjelaskan bahwa dengan semakin banyak teknologi informasi yang digunakan oleh Dinas Komunikasi dan Informatika Kota Batu maka akan semakin banyak juga informasi yang di kelola oleh *server center*. Berdasarkan dalam peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 terkait Sistem Manajemen Pengamanan Informasi, dijelaskan bahwa setiap penyelenggaran sistem elektronik harus menyelenggarakan keamanan terhadap informasi dalam kepentingan umum, pelayanan publik, kelancaran penyelengaraan Negara atau pertahanan dan keamanan Negara. Berdasarkan perturan menteri, pihak Dinas Komunikasi dan Informatika Kota Batu memiliki suatu keharusan untuk mengamankan segala informasi yang dikelolanya. Sebelumnya Dinas Komunikasi dan Informatika telah melakukan *Information Technology Security Assessment* (ITSA) pada aspek celah kerawanan dan keamanan jaringan (*Penetration Test*) yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN). Berdasar penilaian tersebut menyatakan bahwa Dinas Komunikasi dan Informatika Kota Batu berada pada kondisi tingkat kerawanan yang sangat tinggi terhadap keamanan informasi. Dari hasil evaluasi tersebut sudah dilakukan beberapa perbaikan, selanjutnya pada bulan November Pemerintah Kota Batu akan melakukan penilaian Sistem Manajemen Keamanan Informasi yang akan di lakukan oleh BSSN. Sehingga dari permasalahan yang ada, diperlukan sebuah evaluasi terhadap keamanan informasi di Dinas Komunikasi dan Informatika Kota Batu.

Evaluasi tingkat keamanan informasi akan dilakukan dengan menggunakan Indeks Keamanan Informasi (KAMI), Indeks KAMI merupakan *tools* yang dikeluarkan oleh Kementerian Komunikasi dan Informatika untuk menilai kondisi keamanan informasi, dan juga untuk mulai membenahi, membangun dan menerapkan pengamanan informasi. Evaluasi tingkat keamanan informasi menggunakan Indeks KAMI mencakup 5 target area keamanan informasi, yaitu tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja pengelolaan keamanan informasi, pengelolaan aset informasi. Evaluasi menggunakan Indeks KAMI lebih baik apabila dilakukan dua kali dalam setahun sebagai alat untuk melakukan tinjauan ulang kesiapan keamanan informasi sekaligus untuk mengukur keberhasilan perbaikan yang diterapkan, dengan pencapaian tingkat kelengkapan atau kematangan tertentu. Hasil evaluasi Indeks KAMI akan ditinjau ulang dengan ISO 27001, ISO 27001 berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem

Manajamen Keamanan Informasi (SMKI), oleh karena itu perlu adanya peninjauan untuk mengetahui standar manakah yang sudah sesuai dan standar mana yang belum dan juga peneliiti akan memberikan rekomendasi untuk Dinas Komunikasi dan Informatika Kota Batu sesuai standar yang ada pada ISO 27001.

Penelitian sebelumnya tentang evaluasi tata kelola sistem keamanan teknologi informasi menggunakan Indeks KAMI dan ISO 27001 pernah dilakukan di KOMINFO Provinsi Jawa Timur. Hasil evaluasi dengan Indeks KAMI adalah memberikan penilaian pada kelima area pada KOMINFO Provinsi Jawa Timur dan menunjukkan nilai 252, dengan nilai tingkat penggunan sistem elektronik sebesar 22. Dari hasil evaluasi KOMINFO Provinsi Jawa Timur belum dapat dikatakan matang dan sesuai dengan ISO 27001

Maka berlandaskan latar belakang yang telah dijabarkan, perlu diadakan penelitian dengan judul **"Evaluasi Kesiapan Kerangka Kerja Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Batu Dengan Menggunakan Indeks KAMI"**. Hasil dari penelitian diharapkan bisa digunakan oleh Dinas Komunikasi dan Informatika Kota Batu dalam melakukan peningkatan keamanan informasi kedepannya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka dapat dirumuskan masalah sebagai berikut :

1. Bagaimana tingkat keamanan informasi Dinas Komunikasi dan Informatika Kota Batu setelah dilakukan evaluasi dengan menggunakan Indeks KAMI ?
2. Bagaimana hasil tinjaun persyaratan yang ada pada ISO 27001 yang belum terpenuhi dari hasil evaluasi Indeks KAMI ?
3. Bagaimana rekomendasi untuk meningkatkan keamanan informasi pada Dinas Komunikasi dan Informasi Kota Batu ?

1.3 Tujuan

Seperti rumusan masalah yang sudah ditentukan, maka tujuan dari penelitian ini adalah:

1. Mengetahui sejauh mana tingkat keamanan informasi pada Dinas Komunikasi dan Informatika Kota Batu dari hasil evaluasi menggunakan Indeks KAMI
2. Mengetahui persyaratan yang belum memenuhi standar ISO 27001 berdasarkan evaluasi Indeks KAMI
3. Memberikan rekomendasi berdasarkan hasil evaluasi untuk meningkatkan keamanan informasi pada Dinas Komunikasi dan Informasi Kota Batu

1.4 Manfaat

Manfaat dari penelitian ini antara lain:

1. Dapat mengetahui informasi terkait tingkat keamanan informasi pada Dinas Komunikasi dan Informasi Kota Batu.
2. Dapat memberikan hasil rekomendasi terkait pengelolaan keamanan informasi untuk meningkatkan keamanan informasi pada Dinas Komunikasi dan Informasi Kota Batu.

1.5 Batasan Masalah

Batasan masalah di dalam penelitian ini antara lain:

1. Penilaian tingkat keamanan informasi dilakukan menggunakan *tools* Indeks KAMI dengan 2 area, area kategori sistem elektronik dan area keamanan informasi, karena area kategori sistem elektronik dan area keamanan berisi sejumlah pertanyaan terkait penggunaan sistem elektronik dan keamanan organisasi
2. Pemberian rekomendasi untuk hasil evaluasi sesuai dengan standar yang terdapat pada ISO 27001, karena ISO 27001 merupakan standar baku yang diakui secara internasional yang menilai terkait keamanan informasi.

1.6 Sistematika Pembahasan

Berikut ini merupakan urutan sistematika penyusunan laporan ditujukkan untuk memberikan gambaran dan uraian dari laporan skripsi secara garis besar yang meliputi beberapa nan sebagai berikut:

BAB 1 : PENDAHULUAN

Bab ini membahas latar belakang yang digunakan untuk melakukan penelitian, rumusan masalah yang ada pada penelitian, tujuan, batasan masalah, manfaat, dan sistematika penulisan dari penelitian yang dilaku

BAB 2 : LANDASAN KEPUSTAKAAN

Bab ini menjelaskan tentang teori-teori yang digunakan sebagai dasar untuk melakukan penelitian yang diambil dari berbagai sumber atau referensi.

BAB 3 : METODOLOGI PENELITIAN

Bab ini membahas tentang metodologi atau langkah-langkah yang digunakan selama penelitian.

BAB 4 : PENGUMPULAN DATA

Bab ini menjelaskan terkait pengumpulan data penelitian yang dilakukan oleh peneliti

BAB 5 : PEMBAHASAN

Bab ini berisi tentang pembahasan dari bagaimana hasil evaluasi tingkat keamanan informasi pada Dinas Komunikasi dan Informasi Kota Batu berdasarkan hasil pada bab sebelumnya

BAB 6: PENUTUP

Bab ini membahas kesimpulan dan saran dari hasil penelitian yang dilakukan.

BAB 2 LANDASAN KEPUSTAKAAN

2.1 Kajian Pustaka

Penelitian sebelumnya yang dilakukan oleh Edo Rizky (2017), menjelaskan bahwa KOMINFO Provinsi Jawa Timur mempunyai data center yang mengelola informasi dari seluruh layanan dan perangkat pada kantor KOMINFO, selain itu terdapat banyak informasi penting dan berharga yang harus dijaga kerahasiannya dan harus diamankan dengan menggunakan keamanan yang memiliki standar yang jelas. KOMINFO juga akan melakukan sebuah sertifikasi ISO 27001 tentang keamanan informasi. Oleh karena itu dilakukan evaluasi tata kelola sistem keamanan teknologi informasi dengan menggunakan Indeks KAMI dan ISO 27001. Berdasarkan hasil evaluasi yang diperoleh dari penelitian tersebut dijelaskan bahwa kategori sistem elektronik yang digunakan berada pada kategori tinggi dengan skor 22, tingkat kematangan pada setiap area keamanan informasi berada pada tingkat I+ dan secara keseluruhan KOMINFO tidak layak untuk melakukan sertifikasi ISO 27001, karena KOMINFO berada pada area merah dengan total keseluruhan skor rata-rata disetiap area keamanan informasi berjumlah 252.

Pada penelitian yang dilakukan oleh Diah Restu (2015), terdapat beberapa permasalahan yang mendukung dilakukannya evaluasi terkait tingkat kelengkapan dan kematangan keamanan informasi pada divisi PTI yaitu, keinginan untuk meningkatkan keamanan informasi sesuai dengan Standar Nasional Indonesia (SNI), kurangnya kesadaran dari setiap staff PTI PDAM terkait keamanan informasi menyebabkan terjadinya penyalahgunaan wewenang yang dilakukan oleh staf PTI yaitu mengubah sistem operasi yang sudah ditetapkan, selain itu kurangnya pengamanan pada ruang server yang ada di divisi PTI juga turut mendukung dilakukannya evaluasi. Dari penelitian yang sudah dilakukan mengakatan bahwa tingkat kelengkapan keamanan informasi sebesar 325 dan tingkat kematangan berada pada tingkat I+ hal ini menunjukan bahwa sudah ada pemahaman mengenai perlu adanya pengelolaan keamanan informasi akan tetapi masih banyak hambatan yang menghalangi yaitu penerapan langkah pengamanan masih belum teratur, tidak adanya pengawasan, pihak-pihak yang terlibat belum menyadari tanggung jawab atas tugas mereka, pihak pengelola keamanan informasi juga belum menyadari tanggung jawabnya .

Menurut Iqbal dan Ichsan (2013), dalam penelitian mereka manajemen keamanan informasi menjadi sangat penting di era modern saat ini, di mana perkembangan teknologi saat ini telah memudahkan orang dalam memperoleh informasi dan meretasnya. Badan Pendidikan dan Pelatihan Keuangan (BPPK) merupakan organisasi/instansi pemerintah di bawah Kementerian Keuangan. Dalam menjalankan tugasnya, BPPK menyediakan akses intranet dan internet di semua satker BPPK melalui *Wide Area Network* (WAN) Kementerian Keuangan.

Pengguna intranet dan internet dari lingkungan BPPK meliputi; pegawai, peserta diklat, pengajar dan tamu. Pada setiap tahunnya jumlah pengguna terus meningkat hal ini berpotensi meningkatkan ancaman terhadap keamanan informasi BPPK. Berangkat dari hal tersebut mendorong Iqbal dan Ichsan melakukan penelitian terkait keamanan informasi pada BPPK dengan menggunakan Indeks KAMI. Dari analisis yang dilakukan mengatakan bahwa tingkat kelengkapan penerapan SMKI BPPK berada pada level perlu perbaikan, area kuning, dengan total skor 212, kemudian peran/tingkat kepentingan TIK berada pada level sedang dengan skor 21, yang artinya BPPK sudah memiliki pemahaman mengenai perlunya peran TIK dalam membantu organisasi.

Selanjutnya Siga Mustaqim (2014) yang melakukan penelitian pada Kantor Wilayah Ditjen Perbendaharaan Negara Jawa Timur dengan latar belakang berdasar dari Keputusan Menteri Keuangan (KMK) Nomor 479/KMK.01/2010 tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Keuangan, dengan tujuan utama untuk mendapatkan peniliaian mengena pengelolaan keamanan TI, mengetahui tingkat kematangan pengelolaan TI dan mendapatkan rekomendasi berdasarkan hasil analisis tersebut. Dari hasil analisis aspek peran TIK mendapatkan skor 36 dari 48, artinya peran TIK relatif tinggi bagi pelaksanaan perbendaharaan, untuk tingkat kesiapan pengelolaan keamanan informasi mendapatkan skor 337 dari 588, yang artinya masih perlu adanya perbaikan, dan untuk tingkat kematangan seluruh area berada pada level II menuju II+ (selisih 3 poin) artinya sudah ada pemahaman terkait keamanan informasi di Kanwil DJPBN Jawa Timur.

Pada tahun 2017 D. I. Sensuse melakukan penelitian yang membahas mengenai berharganya informasi untuk intansi pemerintah, terutama ketika organisasi tersebut memberikan informasi penting terkait cuaca dan bencana alam. Data dari ID-CERT menunjukan bahwa lebih dari 20.000 laporan terkait dengan pelanggaran keamanan, seperti *spam*, *phising* dan *malware*. Kebutuhan terhadap keamanan informasi menjadi hal yang sangat diperlukan untuk organasi semacam BMKG. Kementerian Komunikasi dan Informatika sudah menyediakan *tools* yang dapat digunakan untuk menilai keamanan informasi suatu organisasi yaitu Indeks KAMI. Indeks KAMI mengacu pada standar baku yaitu ISO, khususnya ISO 27001 tentang Sistem Manajemen Keamanan Informasi. BMKG melakukan penilaian indeks KAMI bertujuan untuk mengidentifikasi bagaimana ketahanan organisasi dan area mana saja yang memerlukan peningkatan keamanan informasi. Hasil yang didapatkan pada tingkat penggunaan TIK, BMKG berada pada level strategis, artinya menunjukan bahwa informasi yang diberikan oleh BMKG dapat memberi dampak besar untuk kondisi Indonesia.

Georg Disterer (2013) melakukan penelitian yang menjelaskan bahwa perusahaan harus tersertifikasi sesuai dengan standar yang ada, dan keamanan informasi dapat didokumentasikan, diterapkan dan dikelola sesuai dengan standar yang diakui secara internasional. Sistem Manajemen Keamanan Informasi (SMKI) yang efektif dapat membantu mengurangi risiko dan mencegah pelanggaran keamanan. Standar ISO 27001 membentuk kerangka kerja untuk merancang dan mengoperasikan SMKI. Dengan ISO/IEC 27001 organisasi dapat menunjukan kepada pelanggan bahwa organisasi "cukup – siap" untuk menyediakan layanan TI yang aman serta memiliki standar yang jelas. Pentingnya sertifikasi keamanan informasi yang sesuai dengan keputusan pengadaan layanan TI akan meningkat dan peningkatan jumlah sertfikasi.

2.2 Profil Dinas Komunikasi dan Inforatika Kota Batu

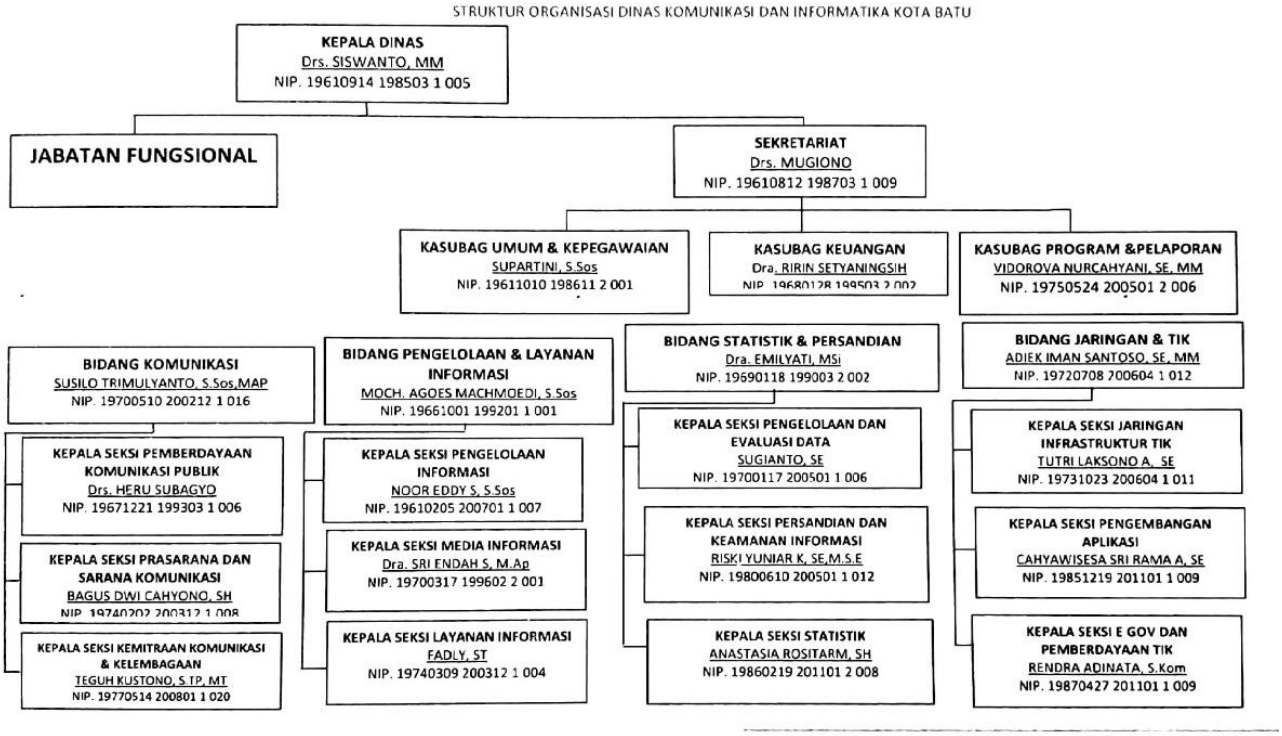
Dinas Komunikasi dan Informatika Kota Batu merupakan suatu bagian dari pemerintahan daerah tepatnya pemerintahan Kota Batu yang mana dalam pejalanannya telah berdiri sejak awal tahun 2017, sebelum Dinas Komunikasi dan Informatika Kota Batu ini berdiri sendiri, pada tahun 2002-2016 Dinas Komunikasi dan Informatika Kota Batu ini merupakan bagian dari Dinas Perhubungan, lalu menginjak awal tahun 2017 Dinas Komunikasi dan Informatika Kota Batu resmi berdiri sendiri sesuai dengan turunnya peraturan Walikota Kota Batu nomor 74 tahun 2016 tentang kedudukan, susunan organisasi, uraian tugas, dan fungsi, serta tata kerja Dinas Komunikasi dan Informatika Kota Batu yang telah menjadi dinas baru.

Dalam kerjanya, Dinas Komunikasi dan Informatika Kota Batu ditugaskan untuk menyediakan data statistik daerah yang valid dan mutakhir, meningkatkan pengamanan informasi dan keamanan daerah yang berklasifikasi dan mewujudkan pelaksanaan sistem informasi dan komunikasi yang terintegrasi, yang mana nantinya diharapkan dapat meningkatkan pengelolaan data secara aktual dan terukur, meningkatnya pengelolaan sistem keamanan informasi yang berklasifikasi meningkatnya pembinaan jaringan komunikasi masyarakat yang berdaya guna dan juga diharapkan akan meningkatkan pengembangan dan pemanfaatan infrastruktur TIK (Teknologi Informasi dan Komunikasi) yang efektif dan merata.

Dinas Komunikasi dan Informatika memiliki visi terwujudnya komunikasi dan informasi yang efektif dan efisien bagi pembangunan masyarakat Kota Wisata Batu, dengan misi meningkatkan keterbukaan dan kemudahan layanan komunikasi dan informasi yang menumbuhkan kreativitas dan inovasi masyarakat bagi pembangunan masyarakat Kota Wisata Batu.

2.2.1 Struktur Organisasi Dinas KOMINFO Kota Batu

Struktur organisasi Dinas Komunikasi dan Informatika adalah sebagai berikut:



Gambar 2. 1 Struktur organisasi Dinas Komunikasi dan Informatika Kota Batu

2.3 Evaluasi

Menurut Kamus Besar Bahasa Indonesia (KBBI) evaluasi adalah upaya penilaian secara teknis dan ekonomis terhadap sesuatu yang dapat digali dan dikembangkan. Pengertian evaluasi yang dikemukakan oleh para ahli yaitu menurut Hadi (2011) dalam bukunya yang berjudul Metode Riset Evaluasi, mendefinisikan evaluasi sebagai "Proses mengumpulkan informasi mengenai objek, menilai objek, dan membandingkanya dengan kriteria, standar dan indikator". Maka dapat ditarik kesimpulan evaluasi merupakan suatu proses untuk menentukan atau menilai seberapa baik performa dari suatu artefak. Artefak dalam evaluasi ini dapat berupa konstruk, model, metode atau instansiasi. Dimana tujuan utama dari evaluasi adalah untuk menghasilkan pengetahuan yang dapat digunakan untuk meningkatkan artefak. Sedangkan tujuan lain dari evaluasi yaitu untuk menyimpulkan bahwa artefak baru harus menyediakan utilitas atau kegunaan yang relatif lebih besar daripada artefak yang ada. Dalam evaluasi sistem informasi, artefak yang dimaksud yaitu sistem informasi berbasis komputer (*computer-based information system*/CBIS) yang

diimplementasikan oleh suatu organisasi. Evaluasi dibagi menjadi tiga jenis, yaitu *goal-based evaluation, goal-free evaluation, criteria-based evaluation*.

Goal – based evaluation, strategi dasar dari pendekatan *goal-based evaluation* adalah untuk mengukur seberapa besar ketercapaian dari tujuan yang telah ditetapkan terpenuhi atau tidak. Pendekatannya menggunakan pendekatan deduktif. Apa yang diukur tergantung pada karakter tujuan dan pendekatan kuantitatif serta pendekatan kualitatif dapat digunakan.

Goal – free evaluation didefinisikan sebagai pengumpulan data sebagai penindak lanjutan atau pemahaman keadaan sistem informasi secara ilmiah atau asli dari pengaruh yang ditimbulkan sistem informasi itu sendiri tanpa berlandaskan tujuan organisasi. Evaluator membuat upaya yang disengaja untuk menghindari semua retorika yang berkaitan dengan tujuan program; tidak ada diskusi tentang tujuan dengan staf; tidak ada proposal program yang dibaca; hanya hasil program dan efek terukur yang dipelajari. Dalam pendekatan ini dibutuhkan keahlian dari evaluator dalam mengevaluasi terkait sistem informasi yang akan divaluasi, sehingga memiliki gambaran permasalahan apa saja yang akan ditemukan dalam proses evaluasi. Strategi dasar dari pendekatan ini adalah evaluasi induktif. Pendekatan ini bertujuan untuk menemukan kualitas objek studi.

Criteria – based evaluation merupakan evaluasi yang berdasarkan pada kriteria, kriteria yang digunakan tidak berasal dari konteks organisasi tertentu tetapi pada perspektif atau teori tertentu. Dalam pendekatan ini diperlukan evaluator yang paham akan standart yang melekat pada sistem informasi, karena standart tersebut nnatinya akan menjadi tolak ukur kegiatan apa saja yang akan dilakukan evaluator selama proses evaluasi berlangsung.

Adapun tahap – tahap yang terdapat dalam evaluasi dibagi menjadi tiga jenis, yaitu tahap perencanaan, tahap pelaksanaan, dan tahap pasca pelaksanaan. Pada tahap perencanaan digunakan untuk mencoba memilih dan menentukan skala prioritas terhadap beberapa alternatif yang ada dan kemungkinan terhadap bagaimana cara mencapai tujuan yang telah di tetapkan sebelumnya. Pada tahap pelaksanaan digunakan untuk melakukan analisa untuk menentukan tingkat kemajuan pelaksanaan dari rencana yang telah ditentukan sebelumnya. Pada tahap pasca pelaksanaan melakukan analisa terhadap objek yang akan dinilai, dimana terdapat dampak apa yang dihasilkan oleh pelaksanaan kegiatan tersebut apakah sesuai dengan tujuan yang ingin dicapai atau tidak.

2.4 Sistem Informasi

Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik. Salah satu jenis sistem elektronik adalah sistem informasi.

Menurut Stair and Reynolds (2018) sistem informasi (SI) merupakan seperangkat komponen yang saling terkait yang mengumpulkan, memproses, menyimpan, dan menyebarluaskan data dan informasi, sistem informasi menyediakan mekanisme *feedback* untuk memonitor dan mengendalikan suatu operasi untuk memastikan operasii tetap memenuhi tujuan dan sasaran. Mekanisme *feedback* sangat penting untuk membantu organisasi mencapai tujuan, seperti meningkatkan laba atau meningkatkan layanan pelanggan.

2.5 Keamanan Informasi

Menurut Tata Sutabri (2012) informasi adalah data yang digunakan untuk pengambilan keputusan dan telah diklasifikasi atau diinterpretasi untuk digunakan dalam proses pengambilan keputusan. Berdasarkan pengertian tersebut maka sebuah keputusan harus diambil berdasarkan data-data yang dikumpulkan dan diklasifikasikan sehingga menghasilkan informasi yang valid, akurat, dan dapat dipertanggung jawabkan guna dimanfaatkan dalam proses pengambilan keputusan untuk sekarang dan keputusan yang akan datang ataupun digunakan untuk pengtahuan.

Keamanan informasi menurut G. J. Simons adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Keamanan informasi menunjukkan masalah bisnis yang menunjukkan suatu organisasi harus melindungi serta menyelesaikan permasalahan keamanan berdasarkan *driver* strateginya sendiri. Hal ini merupakan usaha untuk mengamankan infrastruktur TI dari akses terlarang (John R, 2014).

Dalam merancang sistem keamanan sistem informasi terdapat aspek-aspek keamanan informasi yang perlu di perhatikan. Aspek-aspek tersebut antara lain: *Confidentiality* (Kerahasian), aspek yang menjamin kerahasiaan informasi atau data dan memastikan informasi hanya dapat diakses oleh pihak yang berwenang; *Integrity* (Integritas), aspek yang menjamin data tidak dapat dirubah tanpa ada ijin pihak yang berwenang, menjaga kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang bisa menyebabkan perubahan pada informasi atau data asli. *Availability* (Ketersediaan), aspek yang menjamin bahwa data akan tersedia pada saat dibutuhkan dan menjamin user dapat mengakses informasi tanpa adanya gangguan.

Menurut Whitman & Mattord (2011) informasi merupakan salah satu aset yang penting untuk dilindungi keamanannya. Perusahaan perlu memperhatikan keamanan aset informasinya, kebocoran informasi dan kegagalan pada sistem dapat mengakibatkan kerugian, baik pada sisi finansial maupun produktifitas perusahaan. Keamanan secara umum dapat diartikan sebagai *'quality or state of being secure-to be free from danger'*. Berikut ini merupakan jenis keamanan informasi yaitu, *Physical*

Security, strategi yang memfokuskan untuk mengamankan anggota organisasi, aset fisik, akses tanpa otorisasi dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran; *Personal Security*, strategi yang lebih memfokuskan untuk melindungi orang-orang dalam organisasi; *Operation Security*, strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan ancaman; *Communications Security*, strategi yang bertujuan untuk mengamankan media informasi dan teknologi informasi; *Network Security*, strategi yang memfokuskan pengamanan peralatan jaringan pada data organisasi.

2.6 ISO 27001:2013

International Organization for Standarization (ISO) dan *International Electrotecnical Comission* (IEC) membentuk sistem khusus untuk standarisasi diseluruh dunia. Untuk memberi gambaran awal kepada organisasi terkait sistem manajemen keamanan mereka, ISO dan IEC sudah mengembangkan beberapa Standar 270001 dikembangkan dari standar 27000. Standar 27001 digunakan untuk menetapkan, menerapkan, memelihara dan meningkatkanSistem Manajemen Keamanan Informasi (SMKI) bagi organisasi. Penting untuk diketahui bahwa standar ini bersifat independen terhadap produk teknologi informasi, penggunaan pendekatan manajemen berbasis resiko, dan bangun untuk menjamin supaya kontrol-kontrol keamanan yang dipilih mampu melindungi dan menjaga informasi dari berbagai macam ancaman, dan memberikan keyakinan tingkat keamanan bagi pihak yang berkepentingan. Standar ini dapat digunakan oleh pihak internal dan eksternal untuk menilai kemampuan organisasi untuk memenuhi persyaratan keamanan informasi organisasi mereka.

Struktur ISO/IEC 27001:2013 dibagi menjadi dua bagian besar, yaitu :

A. Klausul : Proses Wajib (*Mandatory Process*)

Klausul (ketentuan/pasal) merupakan persyaratan yang harus dipenuhi apabila organisasi menerapkan SMKI dengan mengacu pada standar ISO/IEC 27001.

Persyaratan utama yang terdapat pada standar ISO 27001:2013 yang harus dipenuhi adalah klausul 0 : *Introduction* (Pendahuluan); klausul 1 : *Scope* (Ruang Lingkup); klausul 2 : *Normatife References* (Rujukan Normatif); klausul 3 : *Terms and Definition* (Istilah dan Definisi); klausul 4 : *Context of Organization* (Konteks Organisasi); klausul 5 : *Leadership* (Kepemimpinan); klausul 6 : *Planning* (Perencanaan); klausul 7 : *Support* (Pendukung); klausul 8 : *Operation* (Operasi); klausul 9 : *Performance Evaluation* (Evaluasi Performa); dan klausul 10 : *Improvement* (Peningkatan).

B. *Annex* A : *Security Control*

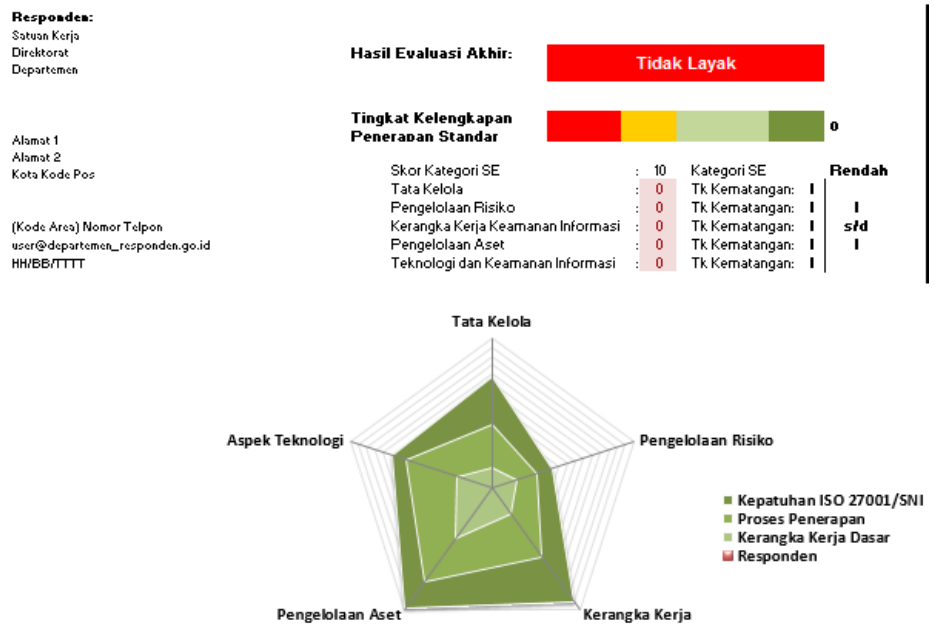
Dari persyaratan tersebut yang merupakan bagian penting dari standar ISO 27001:2013 berada pada klausul 4 hingga klausul 10. Klausul 4 hingga klausul 10 berisi ketentuan, tahapan, proses dan aktivitas yang menjadi kebutuhan yang harus dipenuhi apabila suatu organisasi akan melakukan sertifikasi

Annex A merupakan naskah lampiran yang disediakan dan dapat dijadikan rujukan untuk menentukan kontrol keamanan (*security control*) yang perlu diimplementasikan dalam Sistem Manajemen Keamanan Informasi, yang terdiri dari 14 domain area, 35 kontrol objektif dan 114 kontrol keamanan informasi. Kontrol keamanan informasi terdiri dari 14 area pengaman yaitu : kebijakan keamanan informasi; organisasi keamanan informasi; keamanan sumber daya manusia; manajemen aset; akses kontrol; kriptografi; keamanan fisik dan lingkungan; keamanan operasi; keamanan komunikasi; akuisisi, pengembangan dan pemeliharaan sistem; hubungan pemasok; manajemen insiden keamanan informasi; aspek keamanan informasi menajemen kesinambungan bisnis; dan kepatuhan.

2.7 Indeks Keamanan Informasi (KAMI)

Indeks KAMI merupakan alat evaluasi yang digunakan untuk menganalisis tingkat kesiapan (kelengkapan dan kematangan) pengaman informasi di intansi pemerintah. Indeks KAMI tidak ditujukan untuk menganalisis kelayakan atau efektifitas bentuk pengamanan yang ada melainkan digunakan sebagai perangkat untuk menggambarkan kesiapan kerangka kerja keamanan informasi kepada pimpinan instansi. Indeks KAMI dilakukan untuk mengevaluasi beberapa area penerapan keamanan informasi, dimana ruang lngkup pembahasan didasarkan pada standar 270001, yaitu kategori sistem elektronik, tata kelola keamanan informasi, pengelolaan risiko keamanan inforamsi, kerangka kerja keamanan informasi, pengelolaan aset informasi , teknologi dan keamanan inforamsi

Hasil evaluasi akan memberikan gambaran tingkat kelengkapan penerapan 27001 dan menunjukkan tata kelola keamanan informasi di instansi pemerintah. Sebagai gambaran, hasil evaluasi indeks KAMI dapat dilihat pada Gambar 2.2.



Gambar 2. 2 Tampilan hasil evaluasi Indeks KAMI

Pada evaluasi keamanan inforamsi berdasar Indeks KAMI terdapat dua bagian yaitu, bagian kategori sistem elektronik dan bagian keamanan informasi. Kategori sistem elektronik merupakan penggambaran mengenai bagaimana keadaan sistem elektronik yang digunakan sebagai pendukung proses kerja. Pada Pada bagian keamanan informasi terdapat 5 area.

Area keamanan informasi yang pertama yaitu tata kelola keamanan informasi yang ditujukan untuk menilai tata kelola keamanan informasi dan juga fungsi instansi,tugas dan tanggungjawab pengelolaan keamanan informasi. Area keamanan informasi yang kedua pengelolaan risiko informasi yang ditujukan untuk mengevaluasi penerapan pengelolaan risiko untuk dijadikan dasar penerapan strategi keamanan informasi. Pada area ini juga digunakan untuk mengidentifikasi dan memitigasi risiko supaya risiko tersebut berada pada tingkat yang sesuai dengan kebijakan yang sudah ditetapkan. Aspek keamanan informasi yang ketiga yaitu kerangka kerja keamanan inforamsi yang ditujukan untuk menilai kelengkapan dan kesiapan kerangka kerja (kebijakan dan prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Selain itu bagian ini menilai kompetensi sumber daya manusia. Aspek keamanan inforamsi yang keempat yaitu pengelolaan aset informasi yang ditujukan untuk menilai kelengkapan aset informasi termasuk keseluruhan proses yang bersifat teknis atau administratif. Aspek yang terakhir yaitu teknologi dan keamanan inforamsi yang ditujukan untuk menilai kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

2.8 Hubungan Indeks KAMI dengan ISO 27001

Standar ISO/IEC 27001:2013 mendefinisikan semua aspek keamanan yang dijadikan acuan oleh Indeks KAMI untuk diterapkan dalam berbagai area yang menjadi target penerapan keamanan informasi. Indeks KAMI merangkum 14 sasaran pengendalian yang ada di ISO/IEC 27001:2013 menjadi 5 area evaluasi, untuk mengukur tingkat kematangan SMKI suatu organisasi.

Berdasarkan Gambar 2.3 dapat dijelaskan hubungan area keamanan informasi pada Indeks KAMI dengan sasaran pengendalian pada ISO 27001:2013 :

a. Tata Kelola Keamanan Informasi :

   Pada area ini merupakan area rangkuman dari beberapa penerapan kontrol yang ada pada ISO 27001:2013, yaitu; Kebijakan keamanan informasi, Organisasi keamanan informasi, Keamanan sumberdaya manusia, Keamanan komunikasi, Manajemen insiden keamanan informasi, Aspek keamanan informasi manajeman kesinambungan bisnis, dan Kepatuhan.

b. Pengelolaan Risiko Keamanan Informasi

   Pada area ini merupakan area rangkuman dari beberapa penerapan kontrol yang ada pada ISO 27001:2013, yaitu; Kebijakan keamanan informasi, Organisasi keamanan informasi, Manajemen aset, Manajemen insiden keamanan informasi, Aspek keamanan informasi manajeman kesinambungan bisnis, dan Kepatuhan.

c. Kerangka Kerja Keamanan Informasi

   Pada area ini merupakan area rangkuman dari beberapa penerapan kontrol yang ada pada ISO 27001:2013, yaitu; Kebijakan keamanan informasi, Organisasi keamanan informasi, Keamanan sumberdaya manusia, Keamanan operasi, Keamanan komunikasi, Akuisisi pengembangan dan pemiliharaan sistem, Manajemen insiden keamanan informasi, Aspek keamanan informasi manajeman kesinambungan bisnis, dan Kepatuhan.

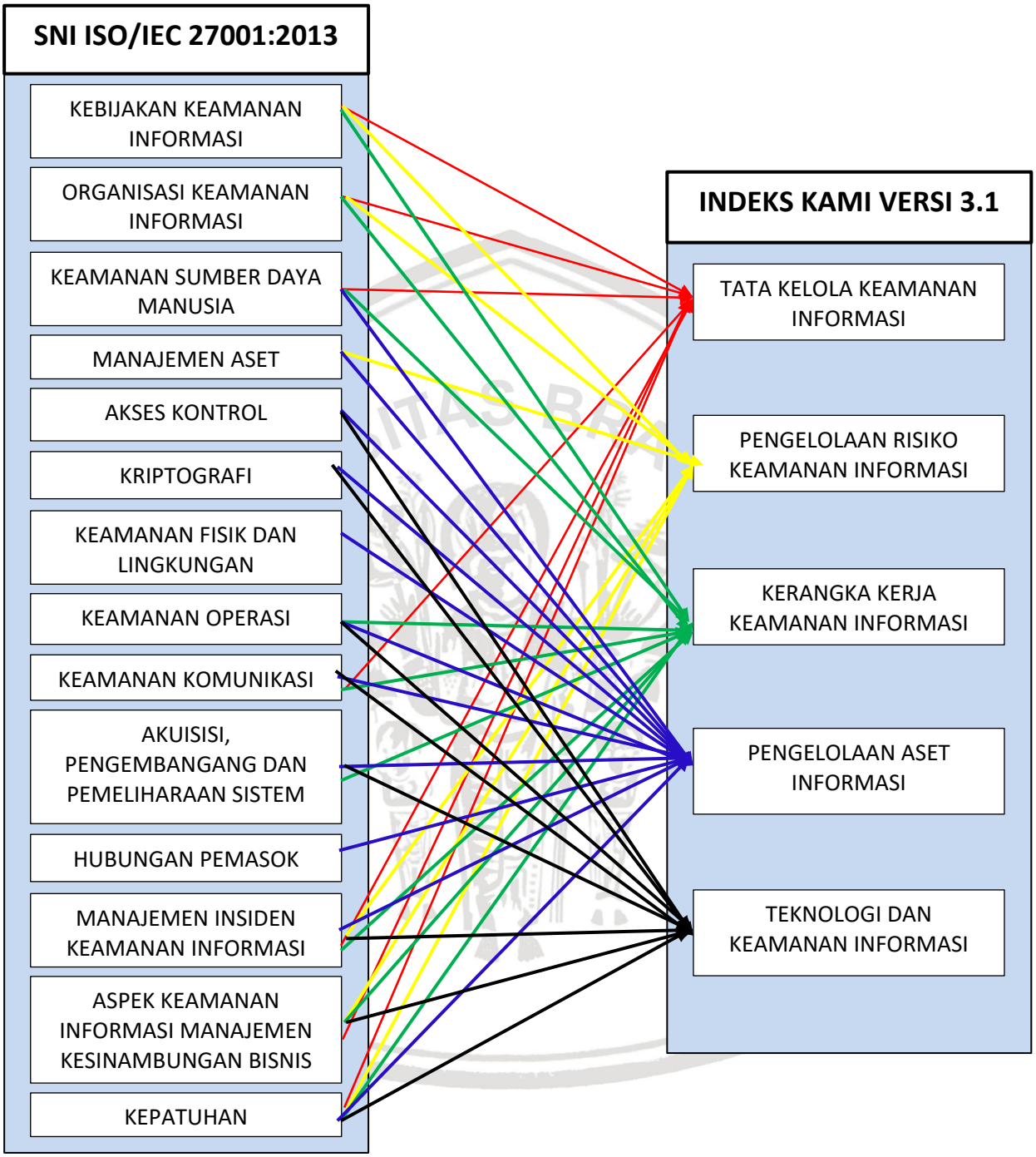
d. Pengelolaan Aset Informasi

   Pada area ini merupakan area rangkuman dari beberapa penerapan kontrol yang ada pada ISO 27001:2013, yaitu; Keamana sumber daya manusia, Manajemen aset, Akses kontrol, Kriptografi, Keamanan Fisik dan Lingkungan, Keamanan operasi, Keamanan komunikasi, Akuisisi pengembangan dan pemiliharaan sistem, Hubungan pemasok, Manajemen insiden keamanan informas, dan Kepatuhan.

e. Teknologi dan Keamanan Informasi

   Pada area ini merupakan area rangkuman dari beberapa penerapan kontrol yang ada pada ISO 27001:2013, yaitu; Akses kontrol, Kriptografi, Keamanan operasi, Keamanan Komunikasi, Akuisisi pengembangan dan pemiliharaan sistem, Manajemen

insiden keamanan informasi, Aspek keamanan informasi manajeman kesinambungan bisnis, dan Kepatuhan.

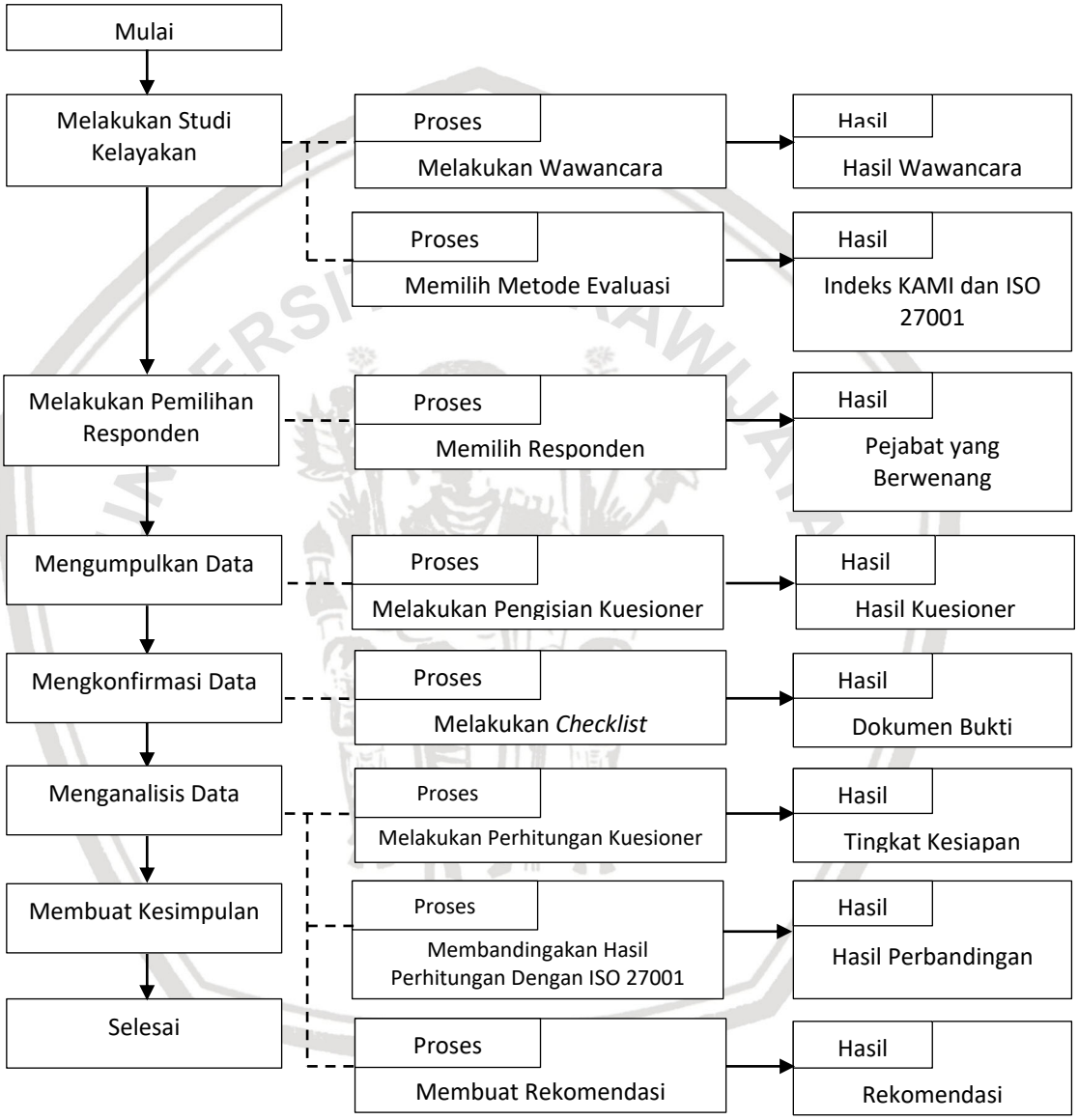


Gambar 2. 3 Hubungan sasaran pengendalian ISO 27001 dengan area pada Indeks KAMI Versi 3.1

BAB 3 METODOLOGI

3.1 Metodologi Penelitian

Metodologi merupakan alur atau tahapan-tahapan yang akan digunakan untuk melakukan penelitian pada Dinas Komunikasi dan Informatika Kota Batu. Penelitian ini merupakan jenis penelitian non implementatif yaitu deskriptif. Metodologi ini menjadikan penelitian menjadi lebih terstruktur dan terarah.



Gambar 3. 1 Alur metode penelitian

Berikut merupakan penjelasan dari Gambar 3.1 alur metode penelitian :

1. Langkah awal yang dilakukan dalam penelitian ini adalah melakukan studi kelayakan, studi kelayakan dilakan dengan wawancara dan studi literatur. Wawancara dilakukan untuk mendapat beberapa informasi, narasumbernya merupakan pejabat yang berada di Dinas Komunikasi dan Informatika Kota Batu. Wawancara dilakukan pada bidang statistik dan persandian, khususnya seksi persandian dan keamanan informasi. Kemudian, melakukan studi literatur dengan membaca jurnal, *paper*, dan buku guna menetukan metode yang cocok untuk melakukan evaluasi. Dan kemudian menentukan metode yang digunakan untuk mengevaluasi yaitu dengan Indekas KAMI dan ISO 27001.
2. Melakukan pemilihan respoden untuk mengisi kuesioner, responden dipilih sesuai dengan panduan yang ada pada Indeks KAMI.
3. Langkah selanjutnya adalah melakukan pengisian kuesioner yang dilakukan oleh Kepala Seksi Persandian dan Keamanan Informasi.
4. Tahapan setelah data kuesioner terkumpul yaitu melakukan validasi data dengan checklist. Validasi ini dilakukan untuk memverifikasi data yang diberikan responden benar-benar sesuai dengan keadaan sebenarnya.
5. Langkah selanjutnya yaitu analisis data. analisis data dilakukan dengan melakukan perhitungan kuesioner dengan menggunakan formula indeks KAMI, lalu melakukan checklist dan diikuti dengan membandingkan hasil evaluasi dengan kontrol yang ada pada ISO 27001 dan membuat rekomendasi
6. Langkah terakhir yang dilakukan yaitu memberikan kesimpulan dan saran untuk DInas Komunikasi dan Informatika Kota Batu

3.2 Melakukan Studi Kelayakan

Pada penelitian ini langkah awal yang dilakukan dalam penelitian adalah dengan melakukan studi kelayakan, studi kelayakan dilakukan dalam du acara, yaitu melakukan wawancara dan studi literatur. Wawancara dilakukan pada bidang statistik dan persandian, khususnya seksi persandian dan keamanan informasi, wawancara ini dilakukan untuk menggali informasi. Metode tanya-jawab (wawancara) dilakukan langsung bertatap muka, untuk mengetahui permasalahan yang akan dibahas. Hasil wawancara akan dijadikan transkip dan divalidasi oleh responden.

Proses selanjutnya yaitu studi literatur, studi literatur dilakukan untuk mencari serta mempelajari jurnal-jurnal terdahulu, pada proses ini didapatkan Indeks KAMI dan ISO 27001.

3.3 Melakukan Pemilihan Responden

Pada tahap ini dilakukan pemilihan responden yang tepat untuk mengisi kuesioner yang akan diberikan. Kriteria responden sendiri dipilih berdasarkan Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks KAMI (2017), responden yang dapat diwawancarai dan mengisi kuesioner yaitu pejabat yang memiliki tanggung jawab dan wewenang untuk mengelola keamanan infomasi.

3.4 Melakukan Pengumpulan Data

Pada tahap ini teknik pengumpulan data yang digunakan pada Dinas Komunikasi dan Informatika Kota Batu adalah dengan melakukan studi lapangan terlebih dahulu, kemudian dilanjutkan dengan penyebaran kuesioner. Kuesioner yang diberikan pada responden mengacu pada Indeks KAMI versi 3.1 yang terdiri dari dua bagian, yaitu kategori sistem elektronik dan area keamanan informasi. Selama pengisian kuesioner peneliti melakukan pendampingan pada semua responden untuk meminimalisir pemalsuan data, setelah itu akan dilakukan ulasan terkait kuesioner yang sudah diisi

Kuesioner pertama yaitu area kategori sistem elektronik seperti yang sudah diijelaskan diatas area ini merupakan penggambaran mengenai bagaimana keadaan sistem elektronik yang digunakan untuk mendukung proses kerja dari instansi. Dalam area kategori sistem elektorni terdapat 10 pertanyaan yang akan digunakan untuk bahan evaluasi.

Bagian I: Kategori Sistem Elektronik			
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan			
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis		**Status**	Skor
#	**Karakteristik Instansi**		
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp. 30 Miliar [B] Lebih dari Rp. 3 Miliar *s/d* Rp. 30 Miliar [C] Kurang dari Rp. 3 Miliar	C	1
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp. 10 Miliar [B] Lebih dari Rp. 1 Miliar *s/d* Rp. 10 Miliar [C] Kurang dari Rp. 1 Miliar	C	1
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	C	1

Gambar 3. 2 Tampilan kuesioner Area I

Sumber: Indeks KAMI Versi 3.1 (2015)

Gambar 3.2 merupakan gambaran terkait kuesioner area satu yang membahas terkait kategori sistem elektronik, dalam tabel tersebut terdapat kolom skor, skor akan berubah apabila *option* yang pada kolom status berubah, skor-skor tersebut akan terakumulasi secara otomatis akhir baris, dari jumlah skor yang di dapatkan akan menggambarkan kategori sistem elektronik, seperti Tabel 3.1.

Tabel 3. 1 Definisi skor Kategori Sistem Elektronik

TOTAL SKOR	**10-15**	**16-34**	**35-50**
KATEGORI SISTEM ELEKTRONIK	RENDAH	TINGGI	STRATEGIS

Sumber: Indeks KAMI Versi 3.1 (2015)

Pada area keamanan informasi terdari dari beberapa area mulai dari area II sampai dengan area VI, yaitu :

a. Area II : Tata Kelola Keamanan Informasi;
b. Area III : Pengelolaan Risiko Keamanan Informasi;
c. Area IV : Kerangka Kerja Pengelolaan Keamanan Informasi;
d. Area V : Pengelolaan Aset Informasi;
e. Area VI : Teknologi dan Keamanan Informasi

Dalam area II sampai dengan area VI berisi sejumlah pertanyaan terkait keamanan informasi, pertanyaan-pertanyaan tersebut dikelompok menjadi tiga kategori pengamanan, dengan ketentuan kategori sebagai berikut :

- Kategori 1 : Berisi pertanyaan yang berhubungan dengan kerangka kerja dasar keamanan informasi.
- Kategori 2 : Berisi pertanyaan yang berhubungan dengan efektfitas dan konsistensi penerapan keamanan informasi.
- Kategori 3 : Berisi pertanyaan yang merujuk pada kemampuan untuk selalu meningkatkan kinerja dari keamanan informasi.

Setiap pertanyaan disetiap area sudah memiliki pilihan opsi jawaban yang sama yaitu terkait status penerapan, berikut merupakan pilihan status penerapan :

- Tidak Dilakukan
- Dalam Perencanaan
- Dalam Penerapan atau Diterapkan Sebagian
- Diterapkan Secara Menyeluruh

Setiap jawaban akan memiliki skor yang berbeda, hal ini berdasarkan tahapan penerapan atau kategori pengamanan. Pada tahapan awal nilainya akan lebih rendah dibandingkan dengan tahapan berikutnya. Hal ini berlaku juga untuk status penerapannya, pada penerapan yang sudah berjalan secara menyeluruh akan memiliki nilai yang lebih tinggi dibandingkan bentuk penerapan lainnya. Hal ini sesuai dengan tingkat kompleksitas yang terlibat dalam proses penerapannya. Tabel pemetaan skor yaitu Tabel 2.2 membentuk matriks antara status penarapan dengan kategori pengamanannya. Apabila jawaban dari kuesioner berstatus "Dalama Perencanaan" dan berada pada kategori pengaman satu maka skor yang didapat adalah satu, jika statusnya "Dalam Perencanaan" dan berada pada kategori pengamanan dua maka skor yang didapat dua, jika statusnya "Dalam Perencanaan" dan berada pada kategori pengamanan tiga maka skor yang didapatkan tiga, begitu pun seterusnya unuk setiap status penerapan dan kategori pengamanan.

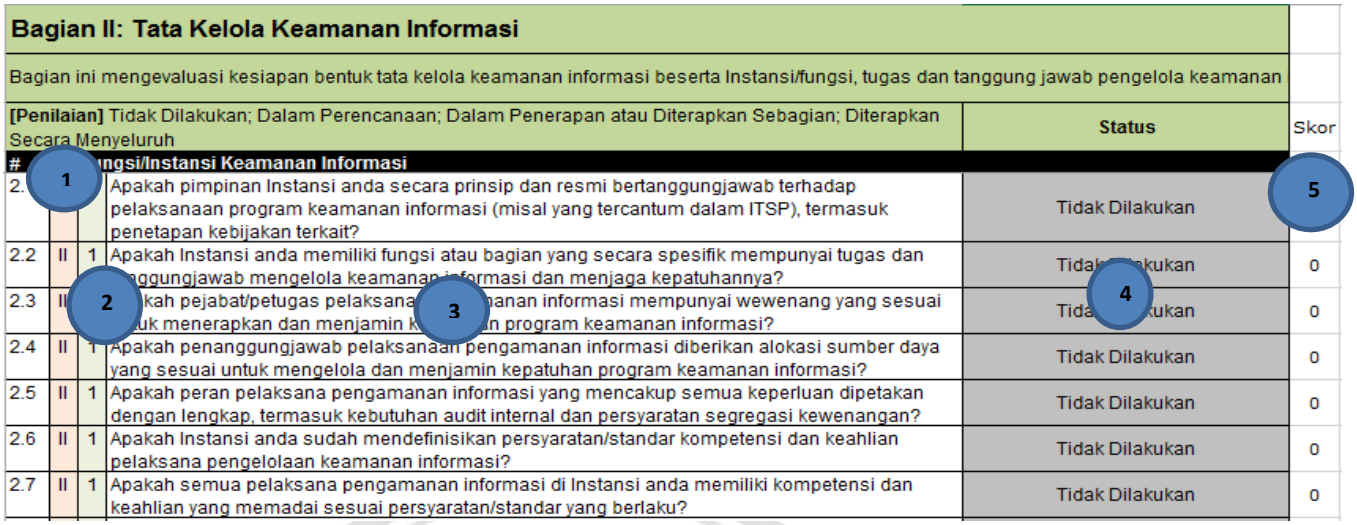
Tabel 3. 2 Pemetaan Kategori Pengamanan

STATUS PENERAPAN	KATEGORI PENGAMANAN		
	1	**2**	**3**
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan Secara Menyeluruh	3	6	9

Sumber: Indeks KAMI versi 3.1 (2015)

Gambar 3.3 merupakan tampilan kuesioner area II sampai dengan area VI, dengan penjelasan mengenai setiap kolom yang terdapat pada table tersebut. Gambar 3.3 manampilkan ilustrasi kuesioner area II sampai area VI, dimana setiap kuesioner memiliki tipe yang sama dengan keterangan sebagai berikut :

1. Tingkat Kematangan
2. Kategori Pengamanan
3. Daftar Pertanyaan
4. Status Penerapan
5. Skor



Bagian II: Tata Kelola Keamanan Informasi

Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan

			[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh	**Status**	Skor
#			**…ngsi/Instansi Keamanan Informasi**		
2.1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Tidak Dilakukan	
2.2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan …nggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Tidak Dilakukan	0
2.3	II	1	…kah pejabat/petugas pelaksana …anan informasi mempunyai wewenang yang sesuai …uk menerapkan dan menjamin k… …n program keamanan informasi?	Tidak Dilakukan	0
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan	0
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Tidak Dilakukan	0
2.6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan	0
2.7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Tidak Dilakukan	0

Gambar 3. 3 Tampilan kuesioner Area II sampai Area VI

Sumber: Indeks KAMI versi 3.1 (2015)

Kuesioner Indeks KAMI Versi 3.1 memiliki total pertanyaan untuk seluruh area keamanan informasi adalah 131 pertanyaan, dengan total skor maksimal 645, dengan keterangan yang dijelaskan dalam Tabel 3.3. Untuk kategori pengaman 1 pada area tata kelola terdapat 8 pertanyaan, area pengelolaan risiko terdapat 10 pertanyaan, area kerangka kerja terdapat 12 pertanyaan, area pengelolaan aset terdapat 24 pertanyaan, area teknologi terdapat 14 pertanyaan. Untuk kategori pengamanan 2 pada area tata kelola terdapat 8 pertanyaan, area pengelolaan risiko terdapat 4 pertanyaan, area kerangka kerja terdapat 10 pertanyaan, area pengelolaan aset terdapat 10 pertanyaan, area teknologi terdapat 10 pertanyaan. Untuk kategori pengamanan 3 pada area tata kelola terdapat 6 pertanyaan, area pengelolaan risiko terdapat 2 pertanyaan, area kerangka kerja terdapat 7 pertanyaan, area pengelolaan aset terdapat 4 pertanyaan, area teknologi terdapat 2 pertanyaan.

Tabel 3. 3 Matriks Kategori Pengaman dan Area Evaluasi

Keterangan	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi
Kategori pengaman 1	8	10	12	24	14
Kategori pengaman 2	8	4	10	10	10
Kategori pengaman 3	6	2	7	4	2
Skor Maksimal	126	72	159	168	120

Tabel 3.4 menggambarkan jumlah pertanyaan yang dipisahkan kedalam masing-masing kategori pengaman dan juga tingkat kematangan keamanan informasi. Seperti tingkat kematangan II dengan kategori pengamanan 1 pada area tata kelola terdapat 8 pertanyaan, area pengelolaan risiko terdapat 10 pertanyaan, area kerangka kerja terdapat 9 pertanyaan, area pengelolaan aset terdapat 24 pertanyaan, dan area tekonologi terdapat 14 pertanyaan, dan begitupun seterusnya untuk tingkat kematangan dan kategori pengamanan lain. Maksimal tingkat kematangan pada kuesioner berada pada tingkat V.

Tabel 3. 4 Jumlah pertanyaan terkait Tingkat Kematangan Keamanan Informasi

Tingkat Kematangan	Keterangan	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi
I						
II	Kategori pengaman 1	8	10	9	24	14
	Kategori pengaman 2	5	0	2	5	0
III	Kategori pengaman 1	0	0	8	0	0
	Kategori pengaman 2	3	2	3	5	10
	Kategori pengaman 3	0	0	2	4	1
IV	Kategori pengaman 2	0	2	0	0	0
	Kategori pengaman 3	6	0	3	0	1
V	Kategori pengaman 3	0	2	2	0	0

3.5 Melakukan Konfirmasi Data

Setelah data terkumpul untuk pengecekan keabsahandata maka dilakukan konfirmasi data, konfirmasi data dilakukan dengan metode triangluasi data. Metode tringaluasi dilakukan dengan mengkombinasikan lebih dari satu Teknik pengumpulan data. Dalam penelitian ini dilakukan dengan cara membandingkan data hasil kuesioner dengan keadaan sebenarnya menggunakan cara *checklist*.

Checklist ini dilakukan dengan cara tatap muka dengan responden yang sudah ditentukan. Dalam tahap ini juga membutuhkan bukti yang didapat dari pertanyaan kuesioner yang terjawab dengan status “Dalam Penerapan/Diterapkan Sebagian” dan “Diterapkan Secara Menyeluruh” pada setiap area.

3.6 Melakukan Analisis Data

Setelah melakukan checklist data, langkah selanjutnya yaitu analisis data dilakukan dengan memasukan jawaban dari responden ke kuesioner pada formula

excel, yang nantinya akan ada dua bentuk hasil, yaitu table penilaian masing-masing area dan diagram radar dengan lima sumbu sesuai area pengamanan.

Hasil setiap penjumlahan skor pada masing-masing area keamanan informasi akan di tampilkan dalam dua instrument, yaitu:

1. Tabel nilai untuk masing-masing area keamanan informasi

Skor Kategori SE	:	10
Tata Kelola	:	0
Pengelolaan Risiko	:	0
Kerangka Kerja Keamanan Informa	:	0
Pengelolaan Aset	:	0
Teknologi dan Keamanan Informas	:	0

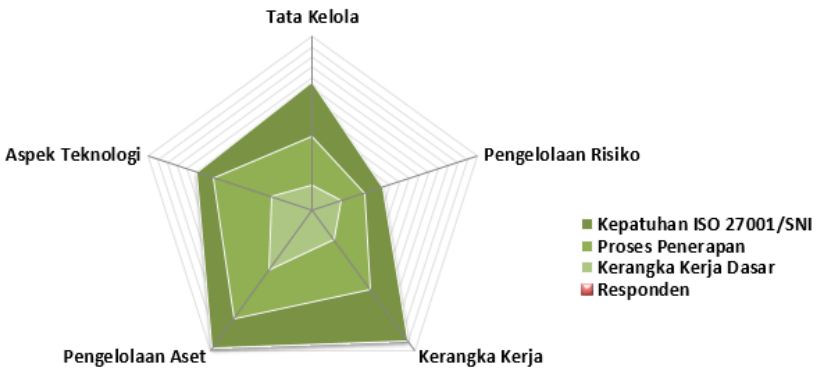
Gambar 3. 4 Skor masing-masing area

Sumber: Indeks KAMI Versi 3.1 (2015)

Gambar 3.4 menunjukkan total skor rata-rata pada masing-masing area yang dievaluasi, nilai ini berguna untuk menghitung nilai akhir dari keamanan informasi instansi.

2. Radar *Chart* dengan lima sumbu yang sesuai dengan area pengamanan

Chart pada Indeks KAMI menggambarkan hubungan antara kepatuhan terhadap standa yang ditetapkan oleh ISO 27001, status penerapan, kerangka kerja dasar, dan skor masing-masing area. Gambar 3.5 merupakan radar chart hasil penilaian keamanan informasi. Ambang batas tingkat kelengakapn (kategori) 1 sampai 3 ditunjukan dengan latar belakang area dengan warna hijau tua sampai hijau muda. Untuk nilai masing-masing area keamanan informasi ditunjukan oleh area yang berwarna merah.



Gambar 3. 5 Radar chart hasil penilaian keamanan informasi

Sumber: Indeks KAMI Versi 3.1 (2015)

Untuk tingkat kematangan informasi terdiri dari 5 tingkatan yaitu :

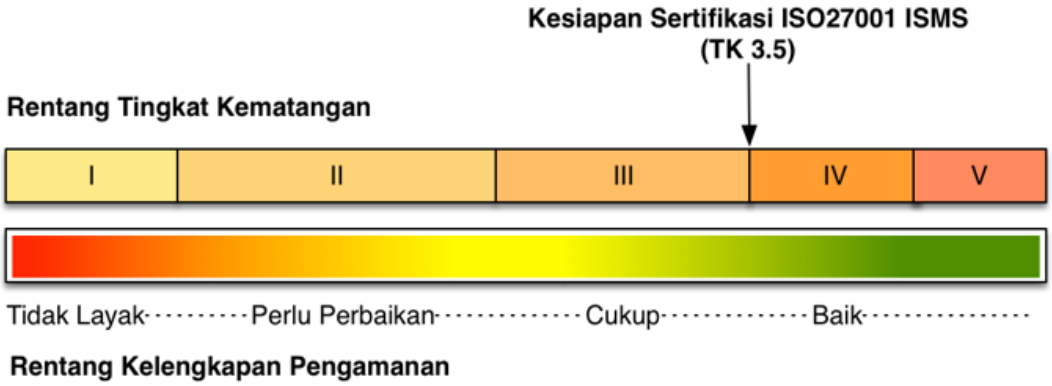
- Tingkat I : Kondisi Awal
- Tingkat II : Penerapan Kerangka Kerja Dasar
- Tingkat III : Terdefinisi dan Konsisten
- Tingkat IV : Terkelola dan Terukur
- Tingkat V : Optimal

Untuk membatu memberikan penilaian yang lebih detail tingkat kematangan dikembangkan menjadi 9 tingkatan, maka pada tingkatan ini ditambahkan dengan tingkatan antara , yaitu ; I+, II+, III+, dan IV+ seperti pada Tabel 3.5. Pada awal penilaian diberikan kategori kematangan Tingkat I. Sebagai ambang batas minimum kesiapan sertifikasi berdasarkan standar ISO/IEC 2700:2013, diperlukan kategori kematangan Tingkat III+ (3,5) atau garis ukur berada pada warna hijau dan dapat dikatan baik seperti pada Gambar 3.6.

Tabel 3. 5 Tingkat kematangan

Level	Tingkat Kematangan
1	I
2	I+
3	II
4	II+
5	III
6	III+
7	IV
8	V+
9	V

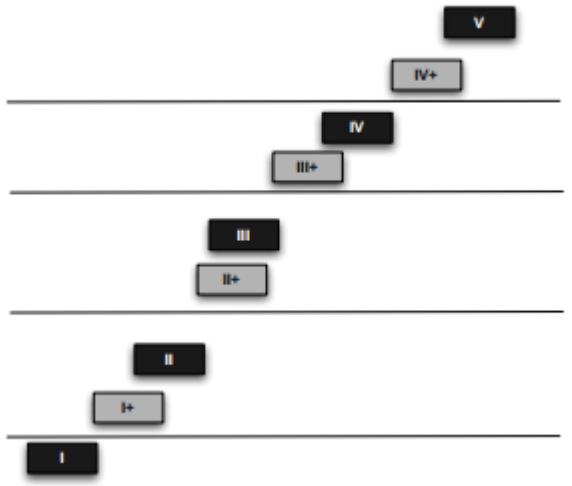
Sumber: Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik (2011)



Gambar 3. 6 Tingkat kesiapan sertifikasi ISO 27001

Sumber: Pengantar Indeks KAMI Versi 3.1 (2015)

Gambar 3.7 merupakan ambang batas pencapaian tingkat kematangan :



Gambar 3. 7 Pencapaian tingkat kematangan

Sumber: Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik (2011)

Untuk mengukur tingkat kesiapan pada kategori sistem elektronik dalam menerapkan SMKI diukur menggunakan tabel berikut sebagai acuan :

KATEGORI SISTEM ELEKTRONIK				
Rendah		Skor Akhir		Status Kesiapan
10	15	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	535	Cukup
		536	645	Baik
Tinggi		Skor Akhir		Status Kesiapan
16	34	0	272	Tidak Layak
		273	455	Perlu Perbaikan
		456	583	Cukup
		584	645	Baik
Strategis		Skor Akhir		Status Kesiapan
35	50	0	333	Tidak Layak
		334	535	Perlu Perbaikan
		536	609	Cukup
		610	645	Baik

Gambar 3. 8 Matriks kategori sistem elektronik dan tingkat kesiapan

Sumber: Pengantar Indeks KAMI Versi 3.1 (2015)

Kemudian untuk mengukur tingkat kelengkapan penerapan ISO 27001 sesuai dengan kategori sistem elektronik diukur dengan menggunakan diagram batang, denga ketentuan apabila garis berada pada warna merah maka statusnya “tidak layak“, apa bila garis berada pada warna kuning berarti status “perlu perbaikan“, dan bila garis berada pada warna hijau maka statusnya “Baik/Cukup”.

3. Membuat Rekomendasi

Setelah melakukan analisis data dari perhitungan Indeks KAMI, kemudian dilakukan penilai terhadap syarat-syarat yang ada pada ISO 27001, dengan cara melakukan perbandingan terhadap syarat-syarat yang terpenuhi dan syarat-syarat yang belum terpenuhi. Syarat-syarat yang belum memenuhi persyaratan ISO 27001 akan diberikan rekomendasi. Rekomendasi dibuat untuk digunakan sebagai acuan bagi organisasi untuk melakukan perbaikan agar keadaan tata kelola keamanan informasi saat ini dapat sesuai dengan standar ISO 27001.

3.7 Kesimpulan

Kesimpulan akan membahas terkait keadaan keamaan informasi saat ini dan keadaan informasii yang diharapkan, dan akan digunakan untuk acuan perbaikan di masa mendatang untuk mencapai tujuan organisasi.

BAB 4 HASIL DAN ANALISIS

4.1 Karakteristik Responden

Kuesioner digunakan untuk mendapatkan hasil atau nilai tingkat kematangan keamanan informasi, kuesioner akan diisi oleh beberapa responden dari dalam instansi, berdasarkan buku Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik (2011), pemilihan responden dipilih berdasar pejabat yang berwenang dan bertanggung jawab sesuai dengan pertanyaan-pertanyaan yang ada pada kuesioner. Tabel 4.1 berisi data responden yang mengisi kuesioner :

Tabel 4.1 Responden kuesioner

No	Nama	Jabatan	Tugas	Keterangan
1.	Cahya Wisesa Sri Rama Atmaja, SE	Kepala Seksi Pengembangan Aplikasi	a. Menyiapkan bahan pelaksanaan program dan kegiatan bidang pengembangan aplikasi. b. Menyiapkan bahan penyusunan kegiatan teknis bidang pengembangan aplikasi. c. Menyiapkan bahan pelaksanaan penerapan aplikasi. d. Melaksanakan pengelolaan dan pengembangan infrastruktur aplikasi dasar/layanan publik/layanan pemerintahan/layanan tata usaha/layana tata laksana dan manajemen aplikasi sistem informasi . e. Melaksanakan pengkoordinasian kebijakan aplikasi informasi di daerah f. Melaksanakan monitoring dan evaluasi pengelolaan aplikasi. g. Melaksanakan pembinaan di bidang aplikasi.	Pada penelitian ini akan mengisi kuesioner pada area Kategori Sistem Elektronik

Tabel 4.1 Responden kuesioner (lanjutan)

No	Nama	Jabatan	Tugas	Keterangan
			h. Melaksanakan monitoring, evaluasi, dan pelaporan kegiatan seksi. i. Melaksanakan tugas lain yang diberikan oleh Kepala Bidang sesuai dengan tugas dan fungsinya.	
2.	Riski Yanuar Kasmilan, SE., M.SE	Kepala Seksi Persandian dan Keamanan Informasi	a. Menyiapkan bahan pelaksanaan program dan kegiatan bidang persandian dan keamanan informasi b. Menyiapkan bahan penyusunan kegiatan teknis bidang persandian dan keamanan informasi c. Menyiapkan bahan koordinasi, sinkronisasi, dan fasilitasi dengan instansi/lembaga terkait dengan persandian d. Menyiapkan bahan pelaksanaan jaringan persandian. e. Menyiapkan bahan penyusunan pedoman dan pelaksanaan persandian. f. Menyiapkan bahan koordinasi, sinkronisasi, dan fasilitasi dengan instansi/lembaga terkait dalam rangka peningkatan dan penguatan persandian dan keamanan informasi. g. Menyiapkan bahan pelaksanaan peningkatan keamanan informasi. h. Menyiapkan bahan analisis dalam upaya penguatan persandian.	Pada penelitian ini akan mengisi kuesioner pada area Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Pengelolaan Keamanan Informasi, Teknologi dan Keamanan Informasi,

Tabel 4.1 Responden kuesioner (lanjutan)

No	Nama	Jabatan	Tugas	Keterangan
			i. Menyiapkan rencana kebutuhan sumber daya manusia sandi. j. Melaksanan pengadaan, penyimpanan, dan distrubusi perangkat lunak dan perangkat keras persandian k. Melaksanakan pemiliharaan dan perbaikan terhadap perangkat lunak persandian, perangkat keras persandian, dan jarigan komunikasi sandi. l. Melaksanakan monitoring, evaluasi, dan pelaporan kegiatan seksi. m. Melaksanakan tugas lain yang diberikan oleh Kepala Bidang sesuai dengan tugas dan fungsinya.	
3.	Robert Eko N. S, S. ST., MT.	Staff Seksi Egovernment , Bidang Jaringan Infrastruktur TIK dan Aplikasi	a. Menyiapkan bahan pelaksanaan program dan kegiatan di bidang pengelolaan *e-government* dan pemberdayaan TIK. b. Menyiapkan bahan penyusunan kebijakan teknis di bidang pengelolaan *e-government* dan pemberdayaan TIK. c. Menyiapkan bahan koordinasi, sinkronisasi dan fasilitasi dengan instansi/lembaga terkait dalam rangka peningkatan *e-government.* d. Menyiapkan bahan analisis dalam penguatan *e-government*.	Pada penelitian ini akan mengisi kuesioner pada area Pengelolaan Aset Informasi

Tabel 4.1 Responden kuesioner (lanjutan)

No	Nama	Jabatan	Tugas	Keterangan
			e. Menyiapkan bahan penyusunan pedoman dan pelaksanaan dalam rangka peningkatan *e-government*. f. Menyiapkan bahan kapasitas masyrakat dalam implementasi tata kelola TIK. g. Melaksanakan monitoring, evaluasi, dan pelaporan *e-government*. h. Melaksanakan kegiatan peningkatan kapasitas sumber daya aparatur bidang TIK. i. Mengelola hosting, layanan domain, sub domain, nama situs SKPD, dan *collcation*. j. Melaksanakan monitoring, evaluasi, dan pelaporan kegiatan seksi. k. Melaksanakan tugas lain yang diberikan oleh Kepala Bidang sesuai dengan tugas dan fungsinya.	

Pada penelitian ini kuesioner yang digunakan adalah kuesioner Indeks KAMI versi 3.1 tahun 2015. Dimana sebelumnya terdapat kuesioner versi 2.2, yang membedakan pada kedua versi adalah jumlah pertanyaan pada setiap area. dan terdapat perubahan nama pada area I, sebelumnya “Peran TIK“ kemudian diganti menjadi “Kategori Sistem Elektronik”.

4.2 Kategori Sistem Elektronik

Kategori sistem elektronik merupakan penggambaran mengenai bagaimana keadaan sistem elektronik yang digunakan untuk mendukung proses kerja dari instansi. Jumlah skor yang didapat adalah 24, berarti bahwa sistem elektronik yang ada pada Dinas Komunikasi dan Informatika Kota Batu termasuk dalam kategori tinggi. Hal ini menjelaskan bahwa proses kerja yang yang berjalan sudah menggunakan sistem elektroni, sehingga menjadi bagian yang tak terpisahkan.

4.3 Tata Kelola Keamanan Informasi

Area tata kelola keamanan informasi ditujukan untuk menilai tata kelola keamanan informasi dan juga fungsi instansi,tugas dan tanggungjawab pengelolaan keamanan informasi. Untuk mendukung hasil dari kuesioner maka dilakukan konfirmasi dengan dilakukan *checklist*, dengan *checklist* ini juga dapat melihat bukti dari keadaan asli apakah sesuai dengan kuesioner. *Checklist* akan dilakukan apabila responden menjawab kuesioner dengan pilihan jawaban "Dalam Penerapan atau Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh", untuk pilihan jawaban selain itu tidak dilakukan *checklist*.

Hasil checklist dari area tata kelola keamanan informasi terdapat 3 (tiga) pertanyaan dengan jawaban "Dalam Penerapan/Diterapkan Sebagian" yang buktinya tidak dapat ditunjukan oleh responden yaitu pertanyaan nomor 2.7, 2.10 dan 2.16, tentang standar pelaksana pengamanan informasi, integrasi keperluan/persyaratan keamanan informasi dalam proses kerja dan kondisi permasalahan keamanan informasi. Seluruh bukti yang ada pada area ini dapat dilihat pada lampiran D.

Berdasarkan hasil kuesioner terdapat lima bentuk pengamanan tingkat kematangan II-Tahap 1 dengan status "Dalam Penerapan/Diterapkan Sebagian" namun terdapat satu pengamanan yang tidak dapat dibuktikan statusnya sehingga menjadi empat bentuk pengamanan tingkat kematangan II-Tahap 1 dengan status "Dalam Penerapan/Diterapkan Sebagian"; terdapat satu bentuk pengamanan tingkat kematangan II-Tahap 1 dengan status "Diterapkan Secara Menyeluruh"; terdapat empat bentuk pengamanan tingkat kematangan II-Tahap 2 dengan status "Dalam Penerapan/Diterapkan Sebagian" namun terdapat satu bentuk pengamanan yang tidak dapat dibuktikan statusnya sehingga menjadi tiga bentuk pengamanan tingkat kematangan II-Tahap 2 dengan status "Dalam Penerapan/Diterapkan Sebagian"; terdapat juga dua bentuk pengamanan tingkat kematangan III-Tahap 2 dengan status "Dalam Penerapan/Diterapkan Sebagian"; terdapat dua bentuk pengamanan tingkat kematangan IV-Tahap 3 dengan status "Dalam Penerapan/Diterapkan Sebagian"; serta sisa jumlah pengamanan tingkat kematangan II-Tahap 1, tingkat kematangan II-Tahap 2, tingkat kematangan III-Tahap 2, tingkat kematangan IV-Tahap 3 yang ada dengan status "Dalam Perencanaan" dan "Tidak Dilakukan" dari peniliaian tingkat kematangan ini sudah mencapai kriteria tingkat kematangan I+, namun belum melampuai kriteria tingkat kematangan II, oleh karena itu area tata kelola keamanan informasi masih berada pada **Level I+**.

4.4 Pengelolaan Risiko Keamanan Informasi

Area pengelolaan risiko informasi yang ditujukan untuk mengevaluasi penerapan pengelolaan risiko untuk dijadikan dasar penerapan strategi keamanan informasi. Pada area ini juga digunakan untuk mengidentifikasi dan memitigasi risiko

supaya risiko tersebut berada pada tingkat yang sesuai dengan kebijakan yang sudah ditetapkan.

Untuk mendukung hasil dari kuesioner maka dilakukan konfirmasi dengan dilakukan *checklist*, dengan *checklist* ini juga dapat melihat bukti dari keadaan asli apakah sesuai dengan kuesioner. *Checklist* akan dilakukan apabila responden menjawab kuesioner dengan pilihan jawaban "Dalam Penerapan atau Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh", untuk pilihan jawaban selain itu tidak dilakukan *checklist*. Berdasarkan hasil kuesioner pada area pengelolaan risiko keamanan informasi tidak dilakukan *checklist*, dikarenakan semua jawaban berstatus "Dalam Perencenaan"

Pada area pengelolaan risiko keamanan informasi dijawab dengan status "Dalam Perencanaan", yang artinya tidak perlu dilakukan *checklist*. Berdasarkan hasil kuesioner seluruh bentuk pengamanan tingkat kematangan II-Tahap 1 berada dalam status "Dalam Perencanaan" yang artinya belum dapat melampaui kriteria tingkat kematangan I+, sehingga dapat disimpulkan area pengelolaan risiko keamanan informasi masih berada pada **Level I**.

4.5 Kerangka Kerja Pengelolaan Keamanan Informasi

Area kerangka kerja keamanan informasi mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Bagian ini juga mengevaluasi tentang kebijakan dan prosedur operasional, kompetensi sumber daya manusia, termasuk juga strategi penerapan, pengukuran efektifitas kontrol dan langkah perbaikan.

Untuk mendukung hasil dari kuesioner maka dilakukan konfirmasi dengan dilakukan *checklist*, dengan *checklist* ini juga dapat melihat bukti dari keadaan asli apakah sesuai dengan kuesioner. *Checklist* akan dilakukan apabila responden menjawab kuesioner dengan pilihan jawaban "Dalam Penerapan atau Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh", untuk pilihan jawaban selain itu tidak dilakukan *checklist*.

Hasil *checklist* dari area tata kelola keamanan informasi terdapat 1 (dua) pertanyaan dengan jawaban "Dalam Penerapan/Diterapkan Sebagian" yang buktinya tidak dapat ditunjukan oleh responden yaitu pertanyaan nomor 4.10, tentang penerapan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*. Seluruh bukti yang ada pada area ini dapat dilihat pada lampiran D.

Berdasarkan hasil kuesioner terdapat tiga bentuk pengamanan tingkat kematangan II-Tahap 1 dengan status "Dalam Penerapan/Diterapkan Sebagian"; terdapat juga tiga bentuk pengamanan tingkat kematangan III-Tahap 1 dengan status "Dalam Penerapan/Diterapkan Sebagian"; terdapat juga lima bentuk pengamanan tingkat kematangan III-Tahap 2 dengan status "Dalam Penerapan/Diterapkan Sebagian" namun terdapat satu bentuk pengamanan yang tidak dapat dibuktikan

statusnya sehingga menjadi empat bentuk pengamanan tingkat kematangan III-Tahap 2 dengan status “Dalam Penerapan/Diterapkan Sebagian”; terdapat satu bentuk pengamanan tingkat kematangan III-Tahap 3 dengan status “Dalam Penerapan/Diterapkan Sebagian”; terdapat dua bentuk pengamanan tingkat kematangan IV-Tahap 3 dengan status “Dalam Penerapan/Diterapkan Sebagian”; dan terdapat dua bentuk pengamanan tingkat kematangan V-Tahap 3 dengan status “Dalam Penerapan/Diterapkan Sebagian” serta sisa jumlah pengamanan tingkat kematangan II-Tahap 1, tingkat kematangan II-Tahap 2, tingkat kematangan III-Tahap 2, tingkat kematangan III-Tahap 3, tingkat kematangan IV-Tahap 3 yang ada dengan status “Dalam Perencanaan” dari peniliaian tingkat kematangan ini sudah mencapai kriteria minimal tingkat kematangan I+, namun belum melampuai kriteria tingkat kematangan II, oleh karena itu area kerangka kerja pengelolaan keamanan informasi masih berada pada **Level I+**.

4.6 Pengelolaan Aset Informasi

Area pengelolaan aset informasi, bagian ini mengevaluasi kelengkapan pengaman terhadap keberadaan aset informasi, termasuk keseluruhan proses yang bersifat teknis ataupun administratif dalam siklus penggunaan aset tersebut. Untuk mendukung hasil dari kuesioner maka dilakukan konfirmasi dengan dilakukan *checklist*, dengan *checklist* ini juga dapat melihat bukti dari keadaan asli apakah sesuai dengan kuesioner. *Checklist* akan dilakukan apabila responden menjawab kuesioner dengan pilihan jawaban “Dalam Penerapan atau Diterapkan Sebagian” dan “Diterapkan Secara Menyeluruh“, untuk pilihan jawaban selain itu tidak dilakukan *checklist*.

Seluruh pertanyaan yang ada pada area pengelolaan aset informasi tersebut dapat menampilkan buktinya, sehingga tidak ada pertanyaan yang harus diturunkan statusnya. Seluruh bukti yang ada pada area ini dapat dilihat pada lampiran D.

Berdasarkan hasil kuesioner terdapat satu bentuk pengamanan tingkat kematangan II-Tahap 1 dengan status “Dalam Penerapan/Diterapkan Sebagian”; terdapat juga satu bentuk pengamanan tingkat kematangan II-Tahap 2 dengan status “Dalam Penerapan/Diterapkan Sebagian”; terdapat juga dua bentuk pengamanan tingkat kematangan III-Tahap 2 dengan status “Dalam Penerapan/Diterapkan Sebagian”, serta sisa jumlah pengamanan tingkat kematangan II-Tahap 1, tingkat kematangan II-Tahap 2, tingkat kematangan III-Tahap 2, tingkat kematangan III-Tahap 3 yang ada dengan status “Dalam Perencanaan” dari peniliaian tingkat kematangan ini sudah mencapai kriteria minimal tingkat kematangan I+, namun belum melampuai kriteria tingkat kematangan II, oleh karena itu area pengelolaan aset informasi masih berada pada **Level I+.**

4.7 Teknologi dan Keamanan Informasi

Area teknologi keamanan informasi mengevaluasi terkait kelengkapan, konsistensi, dan efektifitas penggunaan teknologi dalam pengaman aset informasi. Untuk mendukung hasil dari kuesioner maka dilakukan konfirmasi dengan dilakukan *checklist*, dengan *checklist* ini juga dapat melihat bukti dari keadaan asli apakah sesuai dengan kuesioner. *Checklist* akan dilakukan apabila responden menjawab kuesioner dengan pilihan jawaban "Dalam Penerapan atau Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh", untuk pilihan jawaban selain itu tidak dilakukan *checklist*.

Seluruh pertanyaan yang ada pada area teknologi dan keamanan informasi tersebut dapat menampilkan buktinya, sehingga tidak ada pertanyaan yang harus diturunkan statusnya. Seluruh bukti yang ada pada area ini dapat dilihat pada lampiran D.

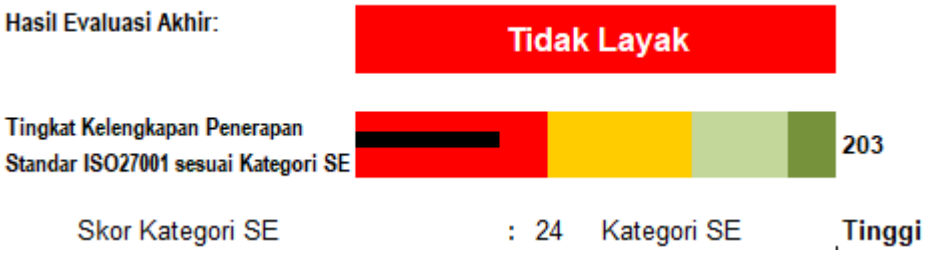
Berdasarkan hasil kuesioner terdapat tujuh bentuk pengamanan tingkat kematangan II-Tahap 1 dengan status "Dalam Penerapan/Diterapkan Sebagian"; terdapat satu bentuk pengamanan tingkat kematangan II-Tahap 1 dengan status "Diterapkan Secara Menyeluruh"; terdapat empat bentuk pengamanan tingkat kematangan III-Tahap 2 dengan status "Dalam Penerapan/Diterapkan Sebagian"; terdapat juga satu bentuk pengamanan tingkat kematangan III-Tahap 3 dengan status "Dalam Penerapan/Diterapkan Sebagian"; terdapat satu bentuk pengamanan tingkat kematangan IV-Tahap 3 dengan status "Dalam Penerapan/Diterapkan Sebagian"; serta sisa jumlah pengamanan tingkat kematangan II-Tahap 1, tingkat kematangan II-Tahap 2, tingkat kematangan III-Tahap 2, tingkat kematangan III-Tahap 3, tingkat kematangan IV-Tahap 3 yang ada dengan status "Dalam Perencanaan" dan "Tidak Dilakukan" dari peniliaian tingkat kematangan ini sudah mencapai kriteria tingkat kematangan I+, namun belum melampuai kriteria tingkat kematangan II, oleh karena itu area teknologi dan keamanan informasi berada pada **Level I+**.

4.8 Hasil Akhir Perhitungan Data Kuesioner

Hasil akhir perhitungan kuesioner akan menunjukan dua hasil penialaian, yang pertama tingkat kelengkapan penerapan keamanan informasi, dan yang kedua tingkat kematangan keamanan informasi.

4.8.1 Tingkat Kelengkapan Penerapan Keamanan Informasi

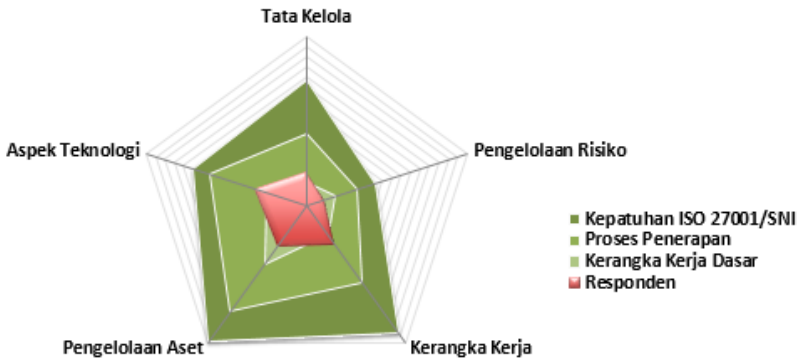
Berdasarkan pengumpulan data penelitian melalui kuesioner dapat dilihat hasil pada tingkat kelengkaan penerapan keamanan informasi Dinas Komunikasi dan Informatika Kota Batu dalam bentu *bar chart* sebagai berikut :



Gambar 4. 1 Tingkat kelengkapan penerapan keamanan informasi Dinas Komunikasi dan Informatika Kota Batu

Berdasarkan gambar 4.1 dapat ditarik kesimpulan bahwa :

a. Pada kategori sistem elektronik, Dinas Komunikasi dan Informatika Kota Batu mendapatkan skor 24, dan termasuk dalam kategori **"Tinggi"**.
b. Sedangkan untuk tingkat kelengkapan penerapan standar ISO27001 sesuai dengan kategori SE mendapatkan skor 203 dan termasuk pada kategori **"Tidak Layak"**, dan berada pada area **"Merah"** .
   Dan untuk tingkat kelengkapan penerapan keamanan informasi dapat dilihat juga pada diagram radar dengan bentuk pentagon berikut :



Gambar 4. 2 Diagram radar tingkat kelengkapan penerapan keamanan informasi

Warna merah pada Gambar 4.2 menjelaskan bahwa kondisikeamanan informasi pada Dinas Komunikasi dan Informatika Kota Batu berdasarkan pengisian kuesioner oleh responden. Dari gambar diatas dapat juga ditarik kesimpulan sebagai berikut :

a. Katagori yang paling baik diantara empat area keamanan informasi adalah kerangka kerja karena paling mendekati standar yang ditetapkan dalam ISO 27001/SNI
b. Kategori yang belum mendakati kerangka kerja dasar dan standar adalah pengelolaan resiko dan pengelolaan aset.

4.8.2 Tingkat Kematangan Keamanan Informasi

Gambar 4.3 menjelaskan tingkat kematangan keamanan informasi Dinas Komunikasi dan Informatika Kota Batu yang ditunjukan dengan bar chart hasil pengumpulan data melalui kuesioner.

Gambar 4. 3 Tingkat kematangan keamanan informasi

Tabel 4.2 Presentase tingkat kematangan keamanan informasi

Keterangan	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi
Skor Maksimal	126	72	159	168	120
Skor Responden	34	18	46	50	55
Presentase	26.9%	25%	28.9%	29.7%	45.8%

Berdasarkan Gambar 4.3 dan Tabel 4.6 tingkat kematangan keamanan informasi Dinas Komunikasi dan Informatika Kota Batu pada masing-masing area adalah sebagai berikut:

a. Tata Kelola Keamanan Informasi
   Skor rata-rata untuk aspek tata kelola keamanan informasi adalah 34 atau 26.9% dari 126 skor maksimal dengan rincian sebagai berikut :
   a) Tingkat kematangan II mendapatkan total skor 28;
   b) Tingkat kematangan III mendapatkan total skor 6; dan
   c) Tingkat kematangan IV mendapatkan total skor 0

Berdasarkan hasil kuesioner yang sudah dilakukan *checklist* didapatkan 3 (tiga) pertanyaan dengan status "Dalam Penerapan/Diterapkan Sebagian" di dalam

kuesioner, yaitu pada pertanyaan nomor 2.7, nomor 2.10, dan nomor 2.16 tidak ada dokumen pendukung, sehingga status penerapannya diturunkan ("Dalam Perencanaan"). Dan terjadi perubahan hasil akhir pada tata kelola keamanan informasi adalah 34 atau 26,9% dan tingkat kematangannya berada pada Level I+.
Pengelolaan Risiko Keamanan Informasi

Skor rata-rata untuk aspek pengelolaan risiko keamanan informasi adalah 18 atau 25% dari 72 skor maksimal dengan rincian sebagai berikut :

a) Tingkat kematangan II mendapatkan total skor 10;
b) Tingkat kematangan III mendapatkan total skor 4;
c) Tingkat kematangan IV mendapatkan total skor 4; dan
d) Tingkat kematangan V mendapatkan total skor 0

Untuk aspek pengelolaan risiko keamanan informasi tidak dilakukan konfirmasi data menggunakan *checklist* karena semua pertanyaan berada pada status "Dalam Perencanaan", sehingga hasil pada aspek pengelolaan risiko adalah tetap 18 atau 25% dan tingkat kematangannya berada pada Level I.

b. Kerangka Kerja Keamanan Informasi

Skor rata-rata untuk aspek kerangka kerja keamanan informasi adalah 46 atau 28,9% dari 159 skor maksimal dengan rincian sebagai berikut :

a) Tingkat kematangan II mendapatkan total skor 16;
b) Tingkat kematangan III mendapatkan total skor 30;
c) Tingkat kematangan IV mendapatkan total skor 0; dan
d) Tingkat kematangan V mendapatkan total skor 0

Berdasarkan hasil kuesioner yang sudah dilakukan *checklist* didapatkan 1 (satu) pertanyaan dengan status "Dalam Penerapan/Diterapkan Sebagian" di dalam kuesioner, yaitu pada pertanyaan nomor 4.10 yang tidak ada dokumen pendukung, sehingga status penerapannya diturunkan ("Dalam Perencanaan"). Dan terjadi perubahan hasil akhir pada kerangka kerja keamanan informasi adalah 46 atau 28.9% dan tingkat kematangannya berada pada Level I+.

c. Pengelolaan Aset Informasi

Skor rata-rata untuk aspek pengelolaan aset informasi adalah 50 atau 29,7% dari 168 skor maksimal dengan rincian sebagai berikut :

a) Tingkat kematangan II mendapatkan total skor 38; dan
b) Tingkat kematangan III mendapatkan total skor 12;

Berdasarkan konfirmasi data menggunakan *checklis*t semua pertanyaan dengan status "Dalam Penerapan/Diterapkan Sebagian" memiliki dokumen pendukung, sehingga hasil akhir dari skor rata-rata pada aspek pengelolaan aset informasi adalahm50 atau 29,7% dan tingkat kematangannya berada pada Level I+.

d. Teknologi dan Keamanan Informasi

Skor rata-rata untuk aspek teknologi dan keamanan informasi adalah 55 atau 45,8% dari 120 skor maksimal dengan rincian sebagai berikut :

a) Tingkat kematangan II mendapatkan total skor 21;
b) Tingkat kematangan III mendapatkan total skor 34;
c) Tingkat kematangan IV mendapatkan total skor 0;

Berdasarkan konfirmasi data menggunakan *checklist* semua pertanyaan dengan status "Dalam Penerapan/Diterapkan Sebagian" memiliki dokumen pendukung, sehingga skor rata-rata pada aspek teknologi dan keamanan informasi adalah 55 atau 45,8% dan tingkat kematangannya berada pada Level I+.

BAB 5 PEMBAHASAN

Berdasarkan hasil penilaian didapatkan bahwa tingkat kelengkapan SMKI pada Gambar 4.1 menunjukkan SMKI kominfo berada pada area merah yang berarti "Tidak Layak". Hal ini menunjukkan bahwa SMKI yang diterapkan saat ini sangat diperlukan perbaikan pada beberapa area keamanan informasi. Beberapa rekomendasi sangat diperlukan untuk meningkatkan SMKI. Rekomendasi yang diberikan didasarkan pada area yang memiliki skor terendah. Urutan yang perlu dilakukan perbaikan yaitu pengelolaan risiko keamanan informasi, tata kelola keamanan informasi, kerangka kerja pengelolaan keamanan informasi, pengelolaan aset informasi dan teknologi & keamanan informasi. Pemberian rekomendasi pada area yang memiliki skor rendah dilakukan dengan membandingkan hasil evaluasi Indeks KAMI dengan kontrol yang terdapat pada SNI ISO/IEC 27001:2013.

5.1 Area Pengelolaan Risiko Keamanan Informasi

Skor rata-rata area pengelolaan risiko keamanan informasi adalah sebesar 18 (25%) dari 72 skor maksimal dan tingkat kematangannya berada pada Level I. Hasil peniliaian memberikan beberapa informasi tentang kondisi pengelolaan risiko keamanan informasi.

Dinas Komunikasi dan Informati Kota batu belum memiliki seperangkat kebijkan dan program kerja terkait keamanan informasi, sehingga diperlukan perbaikan dengan membuat membuat kebijakan dan program kerja terkait keamanan informasi, perbaikan didasarkan oleh kontrol A.5.1.1 pada ISO 27001. Kebijakan keamanan informasi merupakan sebuah infrastruktur keamanan yang harus dimiliki oleh sebuah organisasi atau perusahaan yang ingin melindungi aset informasi terpentingnya. Dokumen ini secara prinsip berisi berbagai cara (baca: kendali) yang perlu dilakukan untuk mengontrol manajemen, mekanisme, prosedur, dan tata cara dalam mengamankan informasi, baik secara langsung maupun tidak langsung. Selain itu Dinas Komunikasi dan Informatika Kota Batu belum memiliki penanggung jawab manajemen risiko, karena belum adanya penanggung jawab manajemen risiko maka perlu menentukan serta mengalokasikan peran dan tanggung jawab sumber daya untuk mengelola keamanan informasi, penentuan dan pengalokasian sumber daya untuk mengelola keamanan informasi didasari oleh kontrol A.6.1.1 pada ISO 27001.

Belum didefinisikannya kepemilikan dan pengelolaan aset informasi yang sudah ada juga menjadi salah satu hasil penilaian, oleh karena itu Dinas Komunikasi dan Informatika Kota Batu perlu mendefinisikan kepemilikan aset yang terdaftar didalam invetaris harus dimiliki supaya sesuai dengan kontrol A.8.1.2 pada ISO 27001. Kemudian persyaratan mitigasi atau penaanggulangan risiko keamanan informasi juga belum di identifikasi, sehingga perlu adanya pembuatan dokumen persyaratan mitigasi risiko yang berkaitan dengan aset yang dimiliki organisasi, pembuatan

dokumen persyaratan mitigasi risiko ada pada kontrol A.15.1.1 pada ISO 27001. Dan hasil penilaiannya lainnya adalah belum adanya ambang batas risiko yang dapat ditangani instansi, karena belum adanya ambang batas risiko maka instanasi harus mencatat dan melaporkan setiap kelemahan keamanan informasi supaya dapat diketahui sejauh mana intansi dapat menangani risiko tersebut, pencatatan dan pelaporan setiap kelemahan keamanan informasi tercantum pada kontrol A.16.1.3 pada ISO

Kondisi yang dihasilkan area pengelolaan risiko keamanan informasi menunjukkan beberapa kekurangan. Rekomendasi yang diberikan untuk kominfo sesuai dengan kontrol- kontrol yang ada dalam kontrol objektif 5.1, 6.1, 8.1, 15.1, dan 16.1 pada ISO 27001:2013 untuk area pengelolaan risiko keamanan informasi.

5.2 Area Tata Kelola Keamanan Informasi

Skor rata-rata area tata kelola keamanan informasi adalah sebesar 34 (26.9%) dari 126 skor maksimal dan tingkat kematangannya berada pada Level I+. Hasil peniliain memberikan informasi tentang kondisi tata kelola keamanan informasi. Pemahaman tentang keamanan informasi di Dinas Komunikasi dan Informatika Kota Batu sudah cukup besar dengan bukti terdapat beberapa program keamanan informasi sudah diterapkan sebagian, melakukan peningkatan kompetensi dan keahlian untuk keamanan informasi. Namun belum terdapat pengamanan informasi dan kebutuhan internal yang dipetakan dengan lengkap, bentuk pengemanan informasi adalah dengan membuat kebijakan terkait keamanan informasi sesuai dengan kontrol A.5.1.1 pada ISO 27001. Kebijakan keamanan informasi merupakan sebuah infrastruktur keamanan yang harus dimiliki oleh sebuah organisasi atau perusahaan yang ingin melindungi aset informasi terpentingnya. Dokumen ini secara prinsip berisi berbagai cara (baca: kendali) yang perlu dilakukan untuk mengontrol manajemen, mekanisme, prosedur, dan tata cara dalam mengamankan informasi, baik secara langsung maupun tidak langsung.

Berdasarkan hasil penilaian pengalokasian sumber daya yang bertanggung jawab dalam pelaksanaan pengamanan informasi masih belum tepat, berdasarkan kontorl A.7.1.1 pada ISO 27001 apabila pengalokasian sumber daya belum tepat, maka diperlukan verifikasi pada semua kandidat sumber daya manusia yang akan dipekerjakan. Dinas Komunikasi dan Informatika Kota Batu belum mengintegrasikan keperluan atau persyaratan keamanan informasi dalam proses kerja, dan belum diterapkan dalam penilaian kerja keamanan infomasi terhadap karyawan. Pada kontrol A.7.2.1 dalam ISO 27001 dijelaskan bahwa seluruh karyawan harus menerapkan keamanan informasi sesuai dengan kebijakan yang sudah ditetapkan.

Selain itu Dinas Komunikasi dan Informatika Kota Batu belum melakukan koordinasi dengan satuan kerja terkait dan pihak eksternal yang berkepentingan untuk menerapkan dan menjamin kepatuhan pengamanan informasi dalam

melakukan transfer informasi, untuk melakukan transfer informasi perlu dibuat kesepakatan mengenai kerjasama dengan satuan kerja yang terlibat sesuai dengan kontrol A.13.2.2 pada ISO 27001. Hasil penilaian lainnya adalah belum adanya pelaporan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi secara rutin dan resmi, sehingga diperlukan pencatatan dan pelaporan setiap kelemahan keamanan informasi, seperti yang tercantum pada kontrol A.16.1.3 pada ISO. Dinas Komunikasi dan Informatika Kota Batu juga belum mendefinisikan kebijakan dan langkah penanggulangan insiden, untuk kedepannya diharapkan dapat merespon insiden sesuai dengan prosedur terdokumentasi sesuai dengan kontrol A.16.1.5 pada ISO 27001. Dinas Komunikasi dan Informatika belum mengidentifikasi legalisasi, perangkat hokum, dan standar terkait keamanan informasi, untuk kedepannya diharapkan pemimpin harus sering melakukan peninjauan terhadap tingkat kepatuhan pemrosesan informasi sesuai dengan kebijakan yang berlaku berdasarkan pada kontrol A.18.2.2 pada ISO 27001.

Kondisi yang dihasilkan area tata kelola keamanan informasi menunjukkan beberapa kekurangan. Rekomendasi yang diberikan untuk kominfo sesuai dengan kontrol- kontrol yang ada dalam kontrol objektif 7.1, 7.2, 13.2, 16.1 dan 18.2 pada ISO 27001:2013 pada ISO 27001:2013 untuk area tata kelola keamanan informasi.

5.3 Area Kerangka Kerja Pengelolaan Keamanan Informasi

Skor rata-rata area kerangka kerja pengelolaan keamanan informasi adalah sebesar 46 (28.9%) dari 159 skor maksimal dan tingkat kematangannya berada pada Level I+. Hasil peniliain memberikan informasi tentang kondisi tata kelola keamanan informasi. Dinas Komunikasi dan Informati Kota batu belum memiliki seperangkat kebijkan dan program kerja terkait keamanan informasi, sehingga diperlukan perbaikan dengan membuat membuat kebijakan dan program kerja terkait keamanan informasi, perbaikan didasarkan oleh kontrol A.5.1.1 pada ISO 27001. Karena belum memiliki kebijakan keamanan informasi, maka belum dilakukan peninjauan terhadap kebijakan keamanan informasi, untuk kedepannya peninjauan terhadap kebijakan keamanan informasi perlu dilakukan sesuai kontrol A.5.1.2 pada ISO 27001.

Dinas Komunikasi dan Informatika Kota Batu belum menerapkan proses pengembangan sistem yang aman (*secure SDLC*), untuk kedepanya diharapkan dapat melakukan pengembangan sistem yang aman (*secure SDLC*) sesuai dengan kontrol ISO A.14.2.1. hasil penilaiannya lainnya adalah belum adanya pelaporan insiden, menjaga kerahasian, Hak Kekayaan Intelektual (HAKI), tata tertib penggunaan dan pengaman aset, berdasarkan kontrol A.16.1.3 pada ISO setiap insiden terkati keamanan informasi harus dicatat dan dilaporkan. Dinas Komunikasi dan Informatika Kota Batu juga belum mengidentifikasikan kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi, untuk kedepanya kondisi yang membahayakan keamanan informasi harus dinilai dan diputuskan apakah

termasuk suatu kejadian keamanan informasi seperti yang tercantum pada kontorl A.16.1.4 pada ISO 27001.

Dinas Komunikasi dan Informatika Kota Batu masih merencanakan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan, dan untuk kedepannya bedasarkan kontrol A.16.1.6 Dinas Komunikasi dan Informatika Kota Batu harus menganalisa dan menyelesaikan insiden keamanan informasi unuk mengurangi kemudian terjadi lagi dimasa depan. Selain itu Dinas Komunikasi dan Informatika Kota Batu belum memiliki kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*), untuk kedepannya disarankan membuat perencanaan keberlanjutan terkait keamanan informasi sesuai dengan kontrol A.17.1.1 pada ISO 27001. Hasil penilaian lainnya adalah belum teridentifikasinya seluruh peraturan yang menyangkut keamanan informasi, perbaikan untuk kedepannyan melakukan identifikasi terhadap perturan perundangan yang berlaku dan persyaratan kontrak sesuai dengan kontrol A.18.1.1 pada ISO 27001.

Kondisi yang dihasilkan area kerangka kerja pengelolaan keamanan informasi menunjukkan beberapa kekurangan. Rekomendasi yang diberikan untuk kominfo sesuai dengan kontrol- kontrol yang ada dalam kontrol objektif 5.1, 14.2, 16.1, 17.1 dan 18.1 pada ISO 27001:2013 untuk area kerangka kerja pengelolaan keamanan informasi.

5.4 Area Pengelolaan Aset Informasi

Skor rata-rata area pengelolaan aset informasi adalah sebesar 50 (29.7%) dari 168 skor maksimal dan tingkat kematangannya berada pada Level I+. Hasil peniliain memberikan informasi tentang kondisi pengelolaan aset informasi. Dinas Komunikasi dan Informatika Kota Batu belum memiliki penanggung jawab pengamanan informasi, karena belum adanya penanggung jawab pengamanan informasi maka perlu menentukan serta mengalokasikan peran dan tanggung jawab sumber daya untuk mengelola keamanan informasi, penentuan dan pengalokasian sumber daya untuk mengelola keamanan informasi didasari oleh kontrol A.6.1.1 pada ISO 27001.

Berdasarkan hasil penilaian proses pengecekan latar belakang sumber daya manusia masih dalam tahap perencanaan, berdasarkan kontorl A.7.1.1 pada ISO 27001 maka diperlukan verifikasi pada semua kandidat sumber daya manusia yang akan dipekerjakan. Belum diterapkannya peraturan dan tata tertib terkait pengamanan penggunaan aset instansi, untuk kedepannya berdasarkan kontrol A.8.1.3 dalam ISO 27001 Dinas Komunikasi dan Informatika diharapkan untuk membuat aturan terkait penggunaan aset instansi.

Selain itu aset informasi juga belum diklasifikasikan sesuai dengan peraturan yang berlaku, berdasarkan kontrol A.8.2.1 dalam ISO 27001 27001 Dinas Komunikasi

dan Informatika diharapkan untuk mengklasifikasikan aset informasi sesuai dengan persyaratan hukum. Pendefinisian tingkat akses yang berbeda dari setiap klasifikasi aset informasi masih dalam tahap perencanaan, untuk kedepannya diharapkan sudah Melakukan pendefinisian tingkat akses dari setiap aset informasi sesuai kontrol A.8.2.2 dalam ISO 27001. Belum adanya proses evaluasi dan klasifikasi aset informasi sesuai tingkat kepentingan, diharapkan untuk kedepannya Dinas Komunikasi dan Informatika Kota Batu bisa mengembangkan dan mengimplementasikan aset informasi sesuai dengan kontrol A.8.2.3 dalam ISO 27001.

Prosedur penggunaan akses (*user access review*) dan hak aksesnya (*user access rights*) masih dalam tahap perencanaan, rekomendasi yang diberikan berdasarkan kontrol A.9.2.2 adalah menyediakan akses penggunaan formal. Untuk pengelolaan identitas elektronik dan proses otentikasi yang masih dalam tahap perencanaan, untuk kedepannya di harapkan Dinas Komunikasi dan Informatika Kota Batu bisa mengontrol alokasi informasi otentikasi sesuai dengan kontrol A.9.2.4 dalam ISO 27001. Dinas Komunikasi dan Informatika Kota Batu belum memiliki prosedur untuk *user* yang mutasi/keluar dari kantor, sehingga rekomendasi yang diberika berdasarkan kontrol A.9.2.6 adalah menghapus hak akses untuk *user* yang mutasi/keluar.

Dinas Komunikasi dan Informatika Kota Batu juga belum memiliki persyaratan dan prosedur pemberian akses, otentikasi, dan otoritas untuk menggunakan aset informasi, dan di sarankan untuk membuat prosedur pemberian akses, otentikasi dan otoritas sesuai dengan kontrol A.9.3.1 dalam ISO 27001. Selain itu belum tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik, rekomendasi yang diberikan adalah melakukan kontrol kunci masuk sesuai dengan kontrol A.11.1.2 dalam ISO 27001. Belum menerapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepetingan/klasfikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang, rekomendasi untuk kedepannya Dinas Komunikasi dan Informatika harus merancang dan menerapkan keamanan fisik untuk kantor, ruangan dan fasilitas sesuai dengan kontrol A.11.1.3 dalam ISO 27001. Konstruksi untuk ruang penyimpanan perangkat pengolahan informasi menggunakan rancangan dan material yang dapat mananggulangi risiko masih dalam tahap perencanaan, untuk kedepannya diharapkan sudah dalam tahap perencanaan untuk merealisasikan kontrol A.11.1.4 dalam ISO 27001 yaitu melindungi aset informasi dari ancaman eksternal dan lingkungan.

Untuk perangkat keras dan fasilitas pendukung Dinas Komunikasi dan Informatika Kota Batu belum memiliki proses untuk memeriksa (inpeksi) dan merawatnya, untuk itu rekomendasinya adalah menerapkan keamanan perlatan dan aset di luar lokasi (kantor) sesuai dengan kontrol A.11.2.4 dalam ISO 27001. Kemudian belum adanya peraturan pengamanan perangkat komputasi apabila digunakan diluar kantor, untuk kedepannya diharapkan Dinas Komunikasi dan Informatika dapat

menerapkan keamanan perlatan dan aset di luar lokasi (kantor) sesuai dengan kontrol A.11.2.6 dalam ISO 27001.

Proses pengelolaan perubahan terhadap sistem, proses bisnis, dan proses teknologi informasi (termasuk perubahan konfigurasi) masih dalam perencanaan, untuk kedepannya apabila proses pengelolaan perubahan sudah dilaksanan, disarankan untuk mengelola setiap perubahan yang dilakukan sesuai dengan kontrol A.12.1.2 dalam ISO 27001. Dinas Komunikasi dan Informatika Kota Batu belum memiliki peraturan terkait instalasi perangkat lunak, rekomendasi untuk kedepannya diharapkan adanya peraturan terkait pembatasan instalasi perangkat lunak sesuai dengan kontrol A.12.6.2 dalam ISO 27001.

Dinas Komunikasi dan Informatika Kota Batu belum memiliki ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya, rekomendasi untuk kedepannya adalah membuat kesepakatan tentang transfer informasi sesuai dengan kontrol A.13.2.2 dalam ISO 27001. Selain itu Dinas Komunikasi dan Informatika Kota Batu belum melakuka proses pelaporan insiden keamanan informasi kepada pihak eksternal atau pihak yang berwajib, untuk kedepannya disarankan untuk melaporkan kejadian keamanan informasi sesuai dengan kontrol A.16.1.2 dalam ISO 27001. Dinas Komunikasi dan Informatika Kota Batu juga belum melakukan proses penyidikan dan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi, rekomendasi untuk kedepannya harus menganalisa dan menyelesaikan insiden keamanan informasi unuk mengurangi kemudian terjadi lagi dimasa depan sesuai dengan kontrol A.16.1.6 dalam ISO 27001

Dinas Komunikasi dan Informatika Kota Batu belum memiliki tata tertib pengaman dan penggunaan aset instansi terkait HAKI, rekomendasi yang disarankan adalah membuat prosedur yang sesuai dengan hak kekayanan intelektual sesuai dengan kontrol A.18.1.2 dalam ISO 27001. Selain itu belum memiliki peraturan terkait penggunaan data pribadi, untuk kedepannya diharapkan ada peraturan terkait penggunaan data dan melakukan perlindungan terhadap informasi indetitas pribadi sesuai dengan kontrol A.18.1.4 dalam ISO 27001. Prosedur *back-up* dan ujicoba pengembalian data (restore) secara berkala masih dalam tahap perencanaan, untuk kedepannya diharapkan Dinas Komunikasi dan Informatika Kota Batu Melakukan peninjauan secara berkala terhadap sistem informasi sesuai dengan kontrol A.18.2.3 dalam ISO 27001.

Kondisi yang dihasilkan area pengelolaan aset informasi menunjukkan beberapa kekurangan. Rekomendasi yang diberikan untuk kominfo sesuai dengan kontrol- kontrol yang ada dalam kontrol objektif 6.1, 7.1, 8.1, 8.2, 9.2, 9.3, 11.1, 11.2, 12.1 12.6, 13.2, 16.1, 18.1 dan 18.2 pada ISO 27001:2013 untuk area pengelolaan aset informasi.

5.5 Area Teknologi dan Keamanan Informasi

Skor rata-rata area teknologi dan keamanan informasi adalah sebesar 55 (45.8%) dari 120 skor maksimal dan tingkat kematangannya berada pada Level I+. Hasil peniliain memberikan informasi tentang kondisi teknologi dan keamanan informasi. Dinas Komunikasi dan Informatika Kota Batu belum memiliki standar konfigurasi untuk keamanan sistem, rekomendasi untuk kedepannya adalah menetapkan kebijakan kontrol akses mengenai konfigurasi keamanan sistem sesuai dengan kontrol A.9.1.1 dalam ISO 27001. Hasil penilaiannya lainnya adalah belum mendukunganya sistem untuk penggantian *password* secara otomatis, sehingga untuk kedepannya diharapkan melakukan manajemen kata sandi sesuai dengan kontrol A.9.4.3 dalam ISO 27001.

Selain belum mendukunganya sistem untuk penggantian *password* secara otomatis, DInas Komunikasi dan Informatika Kota Batu juga belum menerapkan pengamanan untuk mengelola kunci enkripsi, rekomendasi untuk kedepannya adalah melakukan pengelolaan kunci enkripsi sesuai dengan kontrol A.10.1.2 dalam ISO 27001. Kemudian belum adanya peraturan pengamanan perangkat komputasi apabila digunakan diluar kantor, untuk kedepannya diharapkan Dinas Komunikasi dan Informatika dapat menerapkan keamanan perlatan dan aset di luar lokasi (kantor) sesuai dengan kontrol A.11.2.6 dalam ISO 27001.

Dinas Komunikasi dan Informatika Kota Batu belum memiliki rekaman hasil pemutakhiran antivirus dan laporan penyerangan virus yang ditindaklanjuti, rekomendasi untuk kedepannya adalah melakukan kontrol terhadap *malware* dan membuar laporan terkait virus yang ditindaklanjuti sesuai dengan kontrol A.12.2.1 dalam ISO 27001. Selain itu perubahan dalam sistem informasi belum secara otomatis terekam di dalam *log,* maka rekomendasinya adalah melakukan pencatatan terkait kejadian yang merekamm aktivitas sesuai dengan kontrol A.12.4.1 dalam ISO 27001.

Belum ada sinkronisasai waktu yang akurat untuk keseluruhan jaringan, sistem dan aplikasi juga merupakan hasil penilaian pada area teknologi dan keamanan informasi, rekomendasi untuk kedepannya adalah melakukan sinkronisasi waktu sesuai dengan kontrol A.12.4.4 dalam ISO 27001. Dinas Komunikasi dan Informatika Kota Batu belum menerapkan pengamanan untuk mendeteksi dan penggunaan akses jaringan, rekomendasinya adalah membuat mekanisme pengamaanan akses jaringan sesuai dengan kontrol A.13.1.2 dalam ISO 27001.

Setiap aplikasi yang ada di DInas Komunikasi dan Informatika belum memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi, oleh karena itu rekomendasi yang diberikan adalah melakukan analisis dan spesifikasi kebutuhan keamanan informasi sesuai dengan kontrol A.14.1.1 dalam ISO 27001. Dan belum secara rutin menganalisa kepatuhan penerapan konfigurasi standar, untuk kedepannya diharapkan rutin melakukan peninjauan kepatuhan teknis sesuai dengan kontrol A.18.2.3 dalam ISO 27001.

Kondisi yang dihasilkan area teknologi dan keamanan informasi menunjukkan beberapa kekurangan. Rekomendasi yang diberikan untuk kominfo sesuai dengan kontrol- kontrol yang ada dalam kontrol objektif 9.1, 9.4, 10.1, 11.2, 12.2, 12.4, 13.1, 14.1 dan 18.2 pada ISO 27001:2013 untuk area tekonologi dan keamanan informasi.

5.6 Rekomendasi Untuk Dinas Komunikasi dan Informatika Kota Batu

Skor rata-rata area pengelolaan risiko keamanan informasi adalah sebesar 18 (25%) dari 72 skor maksimal dan tingkat kematangannya berada pada Level I. Hasil peniliaian memberikan beberapa informasi tentang kondisi pengelolaan risiko keamanan informasi. Dinas Komunikasi dan Informati Kota batu belum memiliki seperangkat kebijkan dan program kerja terkait keamanan informasi, sehingga diperlukan perbaikan dengan membuat membuat kebijakan dan program kerja terkait keamanan informasi, perbaikan didasarkan oleh kontrol A.5.1.1 pada ISO 27001. Selain itu Dinas Komunikasi dan Informatika Kota Batu belum memiliki penanggung jawab manajemen risiko, karena belum adanya penanggung jawab manajemen risiko maka perlu menentukan serta mengalokasikan peran dan tanggung jawab sumber daya untuk mengelola keamanan informasi, penentuan dan pengalokasian sumber daya untuk mengelola keamanan informasi didasari oleh kontrol A.6.1.1 pada ISO 27001.

Belum didefinisikannya kepemilikan dan pengelolaan aset informasi yang sudah ada juga menjadi salah satu hasil penilaian, oleh karena itu Dinas Komunikasi dan Informatika Kota Batu perlu mendefinisikan kepemilikan aset yang terdaftar didalam invetaris harus dimiliki supaya sesuai dengan kontrol A.8.1.2 pada ISO 27001. Kemudian persyaratan mitigasi atau penaanggulangan risiko keamanan informasi juga belum di identifikasi, sehingga perlu adanya pembuatan dokumen persyaratan mitigasi risiko yang berkaitan dengan aset yang dimiliki organisasi, pembuatan dokumen persyaratan mitigasi risiko ada pada kontrol A.15.1.1 pada ISO 27001. Dan hasil penilaiannya lainnya adalah belum adanya ambang batas risiko yang dapat ditangani instansi, karena belum adanya ambang batas risiko maka instanasi harus mencatat dan melaporkan setiap kelemahan keamanan informasi supaya dapat diketahui sejauh mana intansi dapat menangani risiko tersebut, pencatatan dan pelaporan setiap kelemahan keamanan informasi tercantum pada kontrol A.16.1.3 pada ISO.

Skor rata-rata area tata kelola keamanan informasi adalah sebesar 34 (26.9%) dari 126 skor maksimal dan tingkat kematangannya berada pada Level I+. Hasil peniliain memberikan informasi tentang kondisi tata kelola keamanan informasi. Pemahaman tentang keamanan informasi di Dinas Komunikasi dan Informatika Kota Batu sudah cukup besar dengan bukti terdapat beberapa program keamanan informasi sudah diterapkan sebagian, melakukan peningkatan kompetensi dan keahlian untuk keamanan informasi. Namun belum terdapat pengamanan informasi dan kebutuhan internal yang dipetakan dengan lengkap, bentuk pengemanan

informasi adalah dengan membuat kebijakan terkait keamanan informasi sesuai dengan kontrol A.5.1.1 pada ISO 27001.

Berdasarkan hasil penilaian pengalokasian sumber daya yang bertanggung jawab dalam pelaksanaan pengamanan informasi masih belum tepat, berdasarkan kontorl A.7.1.1 pada ISO 27001 apabila pengalokasian sumber daya belum tepat, maka diperlukan verifikasi pada semua kandidat sumber daya manusia yang akan dipekerjakan. Selain itu Dinas Komunikasi dan Informatika Kota Batu belum melakukan koordinasi dengan satuan kerja terkait dan pihak eksternal yang berkepentingan untuk menerapkan dan menjamin kepatuhan pengamanan informasi dalam melakukan transfer informasi, untuk melakukan transfer informasi perlu dibuat kesepakatan sesuai dengan kontrol A.13.2.2 pada ISO 27001.

Skor rata-rata area kerangka kerja pengelolaan keamanan informasi adalah sebesar 46 (28.9%) dari 159 skor maksimal dan tingkat kematangannya berada pada Level I+. Hasil peniliain memberikan informasi tentang kondisi tata kelola keamanan informasi. Dinas Komunikasi dan Informati Kota batu belum memiliki seperangkat kebijkan dan program kerja terkait keamanan informasi, sehingga diperlukan perbaikan dengan membuat membuat kebijakan dan program kerja terkait keamanan informasi, perbaikan didasarkan oleh kontrol A.5.1.1 pada ISO 27001. Karena belum memiliki kebijakan keamanan informasi, maka belum dilakukan peninjauan terhadap kebijakan keamanan informasi, untuk kedepannya peninjauan terhadap kebijakan keamanan informasi perlu dilakukan sesuai kontrol A.5.1.2 pada ISO 27001.

Hasil penilaiannya lainnya adalah belum adanya pelaporan insiden, menjaga kerahasian, Hak Kekayaan Intelektual (HAKI), tata tertib penggunaan dan pengaman aset, berdasarkan kontrol A.16.1.3 pada ISO setiap insiden terkati keamanan informasi harus dicatat dan dilaporkan. Dinas Komunikasi dan Informatika Kota Batu juga belum mengidentifikasikan kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi, untuk kedepanya kondisi yang membahayakan keamanan informasi harus dinilai dan diputuskan apakah termasuk suatu kejadian keamanan informasi seperti yang tercantum pada kontorl A.16.1.4 pada ISO 27001.

Skor rata-rata area pengelolaan aset informasi adalah sebesar 50 (29.7%) dari 168 skor maksimal dan tingkat kematangannya berada pada Level I+. Hasil peniliain memberikan informasi tentang kondisi pengelolaan aset informasi. Dinas Komunikasi dan Informatika Kota Batu belum memiliki penanggung jawab pengamanan informasi, karena belum adanya penanggung jawab pengamanan informasi maka perlu menentukan serta mengalokasikan peran dan tanggung jawab sumber daya untuk mengelola keamanan informasi, penentuan dan pengalokasian sumber daya untuk mengelola keamanan informasi didasari oleh kontrol A.6.1.1 pada ISO 27001.

Belum diterapkannya peraturan dan tata tertib terkait pengamanan penggunaan aset instansi, untuk kedepannya berdasarkan kontrol A.8.1.3 dalam ISO

27001 Dinas Komunikasi dan Informatika diharapkan untuk membuat aturan terkait penggunaan aset instansi. Selain itu aset informasi juga belum diklasifikasikan sesuai dengan peraturan yang berlaku, berdasarkan kontrol A.8.2.1 dalam ISO 27001 27001 Dinas Komunikasi dan Informatika diharapkan untuk mengklasifikasikan aset informasi sesuai dengan persyaratan hukum. Pendefinisian tingkat akses yang berbeda dari setiap klasifikasi aset informasi masih dalam tahap perencanaan, untuk kedepannya diharapkan sudah Melakukan pendefinisian tingkat akses dari setiap aset informasi sesuai kontrol A.8.2.2 dalam ISO 27001. Belum adanya proses evaluasi dan klasifikasi aset informasi sesuai tingkat kepentingan, diharapkan untuk kedepannya Dinas Komunikasi dan Informatika Kota Batu bisa mengembangkan dan mengimplementasikan aset informasi sesuai dengan kontrol A.8.2.3 dalam ISO 27001.

Untuk pengelolaan identitas elektronik dan proses otentikasi yang masih dalam tahap perencanaan, untuk kedepannya di harapkan Dinas Komunikasi dan Informatika Kota Batu bisa mengontrol alokasi informasi otentikasi sesuai dengan kontrol A.9.2.4 dalam ISO 27001. Dinas Komunikasi dan Informatika Kota Batu juga belum memiliki persyaratan dan prosedur pemberian akses, otentikasi, dan otoritas untuk menggunakan aset informasi, dan di sarankan untuk membuat prosedur pemberian akses, otentikasi dan otoritas sesuai dengan kontrol A.9.3.1 dalam ISO 27001.

Selain itu belum tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik, rekomendasi yang diberikan adalah melakukan kontrol kunci masuk sesuai dengan kontrol A.11.1.2 dalam ISO 27001. Belum menerapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepetingan/klasfikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang, rekomendasi untuk kedepannya Dinas Komunikasi dan Informatika harus merancang dan menerapkan keamanan fisik untuk kantor, ruangan dan fasilitas sesuai dengan kontrol A.11.1.3 dalam ISO 27001. Konstruksi untuk ruang penyimpanan perangkat pengolahan informasi menggunakan rancangan dan material yang dapat mananggulangi risiko masih dalam tahap perencanaan, untuk kedepannya diharapkan sudah dalam tahap perencanaan untuk merealisasikan kontrol A.11.1.4 dalam ISO 27001 yaitu melindungi aset informasi dari ancaman eksternal dan lingkungan.

Kemudian belum adanya peraturan pengamanan perangkat komputasi apabila digunakan diluar kantor, untuk kedepannya diharapkan Dinas Komunikasi dan Informatika dapat menerapkan keamanan perlatan dan aset di luar lokasi (kantor) sesuai dengan kontrol A.11.2.6 dalam ISO 27001. Dinas Komunikasi dan Informatika Kota Batu belum memiliki ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya, rekomendasi untuk kedepannya adalah membuat kesepakatan tentang transfer informasi sesuai dengan kontrol A.13.2.2 dalam ISO 27001. Dinas Komunikasi dan Informatika Kota Batu juga belum melakukan proses penyidikan dan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi,

rekomendasi untuk kedepannya harus menganalisa dan menyelesaikan insiden keamanan informasi unuk mengurangi kemudian terjadi lagi dimasa depan sesuai dengan kontrol A.16.1.6 dalam ISO 27001

Dinas Komunikasi dan Informatika Kota Batu belum memiliki tata tertib pengaman dan penggunaan aset instansi terkait HAKI, rekomendasi yang disarankan adalah membuat prosedur yang sesuai dengan hak kekayanan intelektual sesuai dengan kontrol A.18.1.2 dalam ISO 27001. Selain itu belum memiliki peraturan terkait penggunaan data pribadi, untuk kedepannya diharapkan ada peraturan terkait penggunaan data dan melakukan perlindungan terhadap informasi indetitas pribadi sesuai dengan kontrol A.18.1.4 dalam ISO 27001. Prosedur *back-up* dan ujicoba pengembalian data (restore) secara berkala masih dalam tahap perencanaan, untuk kedepannya diharapkan Dinas Komunikasi dan Informatika Kota Batu Melakukan peninjauan secara berkala terhadap sistem informasi sesuai dengan kontrol A.18.2.3 dalam ISO 27001.

Skor rata-rata area teknologi dan keamanan informasi adalah sebesar 55 (45.8%) dari 120 skor maksimal dan tingkat kematangannya berada pada Level I+. Hasil peniliain memberikan informasi tentang kondisi teknologi dan keamanan informasi. Dinas Komunikasi dan Informatika Kota Batu belum memiliki standar konfigurasi untuk keamanan sistem, rekomendasi untuk kedepannya adalah menetapkan kebijakan kontrol akses mengenai konfigurasi keamanan sistem sesuai dengan kontrol A.9.1.1 dalam ISO 27001. Kemudian belum adanya peraturan pengamanan perangkat komputasi apabila digunakan diluar kantor, untuk kedepannya diharapkan Dinas Komunikasi dan Informatika dapat menerapkan keamanan perlatan dan aset di luar lokasi (kantor) sesuai dengan kontrol A.11.2.6 dalam ISO 27001.

Selain itu perubahan dalam sistem informasi belum secara otomatis terekam di dalam *log,* maka rekomendasinya adalah melakukan pencatatan terkait kejadian yang merekamm aktivitas sesuai dengan kontrol A.12.4.1 dalam ISO 27001. Dan belum secara rutin menganalisa kepatuhan penerapan konfigurasi standar, untuk kedepannya diharapkan rutin melakukan peninjauan kepatuhan teknis sesuai dengan kontrol A.18.2.3 dalam ISO 27001.

BAB 6 PENUTUP

6.1 Simpulan

Dari hasil penelitian keamanan informasi yang dilakukan pada Dinas Komunikasi dan Informatika Kota Batu didapatkan kesimpulan sebagai berikut:

1. Dinas Komunikasi dan Informatika Kota Batu berada pada kategori rendah dengan skor 203 untuk tingkat kelengkapan, karena belum menerapkan semua syarat keamanan informasi atau masih dalam tahap perencanaan. Sedangkan untuk tingkat kematangan setiap area keamanan informasi berada pada Level I sampai Level I+.
2. Hasil analisis menunjukan beberapa kontrol ISO 27001:2013 yang belum terpenuhi berdasarkan masing-masing area keamanan informasi pada Indeks KAMI, antara lain area tata kelola keamanan informasi berada pada kontrol A.5.1.1, A.7.1.1, A.7.2.1, A.13.2.2, A.16.1.3, A.16.1.5, A18.2.2; area pengelolaan risiko keamanan informasi berada pada kontrol A.5.1.1, A.6.1.1, A.8.1.2, A.15.1.1, dan A.16.1.3; area kerangka kerja keamanan informasi berada pada kontrol A.5.1.1, A.5.1.2, A.14.2.1, A.16.1.3, A.16.1.4, A.16.1.6, A.17.1.1, dan A.18.1.1; area pengelolaan asset informasi berada pada kontrol A.6.1.1, A.7.1.1, A.8.1.3, A.8.2.1, A.8.2.2, A.8.2.3, A.9.2.2, A.9.2.4, A.9.2.6, A.9.3.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.2.4, A.11.2.6, A.12.1.2, A.12.6.2, A.13.2.2, A.16.1.2, A.16.1.6, A.18.1.2, A.18.1.4 dan A.18.2.3; area teknologi dan keamanan informasi berada pada kontrol A.9.1.1, A.9.4.3, A.10.1.2, A11.2.6, A.12.2.1, A.12.4.1, A.12.4.4, A.13.1.2, A.14.1.1, dan A.18.2.3.
3. Berdasarkan hasil analisis, untuk meningkatkan tingkat kelengkapan dan kematangan keamanan informasi, maka Dinas Komunikasi dan Informatika Kota Batu mendapatkan beberapa rekomendasi diantaranya sebagai berikut :
    a. Pengelolaan risiko keamanan informasi berada pada tingkat kematangan I, untuk dapat mencapai tingkat kematangan II maka Dinas Komunikasi dan Informatika perlu membuat kebijakan dan program kerja terkait keamanan informasi; menentukan serta mengalokasikan peran dan tanggung jawab sumber daya untuk mengelola keamanan informasi; mendefinisikan kepemilikan aset yang terdaftar didalam invetaris harus dimiliki; perlu adanya pembuatan dokumen persyaratan mitigasi risiko yang berkaitan dengan aset yang dimiliki organisasi; mencatat dan melaporkan setiap kelemahan keamanan informasi supaya dapat diketahui sejauh mana intansi dapat menangani risiko tersebut.
    b. Tata kelola keamanan informasi berada pada tingkat kematangan I+, untuk dapat mencapai tingkat kematangan II maka Dinas Komunikasi dan Informatika perlu membuat kebijakan dan program kerja terkait keamanan

informasi; diperlukan verifikasi pada semua kandidat sumber daya manusia yang akan dipekerjakan; untuk melakukan transfer informasi perlu dibuat kesepakatan dengan pihak yang bersangkutan.

c. Kerangka kerja pengelolaan keamanan informasi berada pada tingkat kematangan I+, untuk dapat mencapai tingkat kematangan II maka Dinas Komunikasi dan Informatika perlu membuat kebijakan dan program kerja terkait keamanan informasi; untuk kedepannya peninjauan terhadap kebijakan keamanan informasi perlu dilakukan; setiap insiden terkait keamanan informasi harus dicatat dan dilaporkan; kondisi yang membahayakan keamanan informasi harus dinilai dan diputuskan apakah termasuk suatu kejadian keamanan informasi.

d. Pengelolaan aset informasi berada pada tingkat kematangan I+, untuk dapat mencapai tingkat kematangan II maka Dinas Komunikasi dan Informatika perlu menentukan serta mengalokasikan peran dan tanggung jawab sumber daya untuk mengelola keamanan informasi; membuat aturan terkait penggunaan aset instansi; mengklasifikasikan aset informasi sesuai dengan persyaratan hukum; melakukan pendefinisian tingkat akses dari setiap aset informasi; mengembangkan dan mengimplementasikan aset informasi; mengontrol alokasi informasi otentikasi; membuat prosedur pemberian akses, otentikasi dan otoritas; melakukan kontrol kunci masuk; merancang dan menerapkan keamanan fisik untuk kantor, ruangan dan fasilitas; melindungi aset informasi dari ancaman eksternal dan lingkungan; menerapkan keamanan perlatan dan aset di luar lokasi (kantor); membuat kesepakatan tentang transfer informasi; menganalisa dan menyelesaikan insiden keamanan informasi unuk mengurangi kemudian terjadi lagi dimasa depan; membuat prosedur yang sesuai dengan hak kekayanan intelektual; membuat peraturan terkait penggunaan data dan melakukan perlindungan terhadap informasi indetitas pribadi; melakukan peninjauan secara berkala terhadap sistem informasi.

e. Teknologi dan keamanan informasi berada pada tingkat kematangan I+, untuk dapat mencapai tingkat kematangan II maka Dinas Komunikasi dan Informatika perlu menetapkan kebijakan kontrol akses mengenai konfigurasi keamanan sistem; menerapkan keamanan perlatan dan aset di luar lokasi (kantor); melakukan pencatatan terkait kejadian yang merekamm aktivitas; melakukan peninjauan kepatuhan teknis.

6.2 Saran

Saran untuk penelitiannya selanjuatnya adalah sebagai berikut :

1. Penelitian sebaiknya dilakukan dengan menggunakan responden yang lebih kompeten, sesuai dengan tugas dan jawab, dan melihat latar belakang

pendidikannya agar dapat mengerti lebih jelas tentang kondisi keamanan informasi.

2. Sebaiknya dilakukan evaluasi ulang apabila rekomendasi pada penelitian ini sudah diimplementasikan, supaya dapat mengetahui perkembagan tingkat kematangannya.
3. Untuk penelitian selanjutnya disarankan melakukan evaluasi menggunakan kerangka kerja lain untuk memperkaya rekomendasi dari peneilitian ini, seperti COBIT 5 pada aspek APO 13 untuk mengukur keamanan informasi dari sisi yang berbeda.

DAFTAR REFERENSI

Afrianto, I., Suryana, T., & Sufa'atin., 2015. *Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI – SNI ISO/IEC 27001:2009 (Studi Kasus Perguruan Tinggi X).* Unikom.

Disterer, G., 2013. *ISO/IEC 27000, 27001, 27002 for Information Security Management.* Journal of Information Security. University of Apploed Science and Arts.

Hadi, Samsul. 2011. *Metode Riset Evaluasi*. Yogyakarta: Penerbit Laksbang Grafika.

Menteri Komunikasi dan Informatika Republik Indonesia. 2016. *Peraturan Menteri Komunikasi dan Informatkia Republik Indonesia Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi*. Peraturan Menteri. Jakarta.

Pratama, E.R., Suprapto., & Perdanakusuma, A.R., 2018. *Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur)*. Jurnal Pengembangan Teknologi Informasidan Ilmu Komputer, 2(11), pp. 5911-5920.

Rencana Kerja (RENJA) Dinas Komunikasi dan Informatika Kota Batu tahun 2018

Rencana Strategis (RENSTRA) Dinas Komunikasi dan Informatika Kota Batu tahun 2017

Sensuse, D.I., Syarif, M., Suprapto, H., Wirawan, R., Satria, D., Normandia, Y., 2017. *Information security evaluation using KAMI index for security improvement in BMKG*, in: 2017 5th International Conference on Cyber and IT Service Management, CITSM 2017. Institute of Electrical and Electronics Engineers Inc.

Siga, M., Susanto, T.D., & Hidayanto, B.C., 2014. *Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi Pada Kantor Wilayah Ditjen Perbendaharaan Negara Jawa Timur.* Institut Teknologi Sepuluh November.

Soenardi, I., & Ichsan, M. 2013. *Analisis Kematangan Sistem Manajemen Keamanan Informasi Badan Pendidikan dan Pelatihan Keuangan Diukur Menggunakan Indeks Keamanan Informasi.* Kajian Akademis BPPK.

Sutabri, Tata. 2012. *Konsep Sistem Informasi*. Yogyakarta: Penerbit Andi.

Tim Direktorat Keamanan Informasi kementerian Komunikasi dan Informatika RI, 2011. *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik*. KOMINFO.

Tim Direktorat Keamanan Informasi kementerian Komunikasi dan Informatika RI, 2017. *Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (KAMI)*. KOMINFO.

Vacca, John R. 2014. *Managing Information System (Second Edition)*. Elsevier. Amsterdam.

Wardani, D.R., & Pujiono., 2015. *Evaluasi Keamanan Informasi Pada PTI PDAM Tirta Moedal Kota Semarang Berdasarkan Indeks Keamanan Informasi SNI ISO 27001:2009.* Techn.COM, 14(3), pp. 165-172

Whitman, Michael E., & Herbert J Mattord. 2012. *Management of Information Security*. Cengage Learning.